California High-Speed Rail Authority

RFP No.: HSR 13-57

Request for Proposal for Design-Build Services for Construction Package 2-3

Book IV, Part D.5 – Safety and Security Management Plan

CALIFORNIA HIGH-SPEED TRAIN SYSTEM

CHSTS SAFETY AND SECURITY MANAGEMENT PLAN

Revision 1

Approved by: Jon Tapping, Risk Manager — Date: 3-25-14

Approved by: Frank Vacca, Chief Program Manager — Date: 4-18-2014

Released by: Jeff Morales, Chief Executive Officer — Date: 4-22-14

Document	Sections/Pages Affected	Date of Document
Rev 0.0	Initial Draft	06/30/11
Rev 0.1	2ND Draft	01/06/2012
Rev 0.2	3rd Draft – FRA Comments, Security Update, S/S Policy, Committee charters, changes in Authority structure	02/14/2013
Rev 1	Revised to reflect new hazard management principles and processes, new Authority organizational structure, and new construction requirements for safety and security	03/04/2014

TABLE OF CONTENTS

[VRuiz1]

FIGURES

TABLES

APPENDICES

ACRONYMS AND ABBREVIATIONS

Acronym or Abbreviation	Definition
ARHRAM	Adjacent Railroad Hazard Risk Assessment Model
Authority	California High-Speed Rail Authority
CEHL	Certifiable Elements and Hazards Log
CFR	Code of Federal Regulations
CHST	California High-Speed Train
CHSTS	California High-Speed Train System
CIL	Critical Items List
CPUC	California Public Utilities Commission
DHS	Department of Homeland Security
EMT	Engineering Management Team
FD	Final Design Phase
FLSSC	Fire/Life Safety and Security Committee
FMEA	Failure Mode Effects Analysis
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
FTAn	Fault Tree Analysis
ICS	Initial Construction Segment
OHA	Operating Hazard Analysis
OMT	Operations and Maintenance Team
PCM	Project Construction Management
PE	Preliminary Engineering Phase
PHA	Preliminary Hazard Analysis
PMO	Program Management Oversight
PMP	Project Management Plan
PMT	Program Management Team
PTEPP	Passenger Train Emergency Preparedness Plan
QC	Quality Control
RAC	Rail Activation Committee
RAP	Rail Activation Plan

RC	Regional Consultant
SITC	System Integration Testing Committee
SONO	Statement of No Objection
SSCP	Safety and Security Certification Plan
SSEC	Safety and Security Executive Committee
SSecPP	System Security Program Plan
SSPP	System Safety Program Plan
SHEA	Software Hazard Effects Analysis
SiSHA	Site-Specific Hazard Analysis
SSHASP	Site-Specific Health and Safety Plan
SSI	Sensitive Security Information
SSMP	Safety and Security Management Plan
SSPC	Safety and Security Program Committee
SSSP	Site-Specific Security Plan
TSA	Transportation Security Administration
TVA	Threat and Vulnerability Assessment
V&V	Verification and Validation

REFERENCE DOCUMENTS

The following documents are referenced in this SSMP:

- 49 CFR Parts 200-299, Federal Railroad Administration regulations
- 49 CFR Part 633, Federal Transit Administration *Project Management Oversight*
- 49 CFR Part 659, Federal Transit Administration *State Safety Oversight*
- ANZI Z590.3-2011 *Prevention through Design*, 01/23/2012
- California Code of Regulations Title 8 Construction Safety Orders
- Department of Defense Military Standard 882E *Standard Practice for System Safety*, 5/11/2012
- European Railway Agency *Common Safety Method on Risk Evaluation and Assessment,* Official Journal of the European Union, 29.4.2009, Regulation 352/2009/EC
- European Railway Agency *Guide for the Application of the CSM Regulation*, ERA/GUI/01-2008/SAF, Version 1.1, page 26
- FRA *Collision Hazard Analysis Guide: Commuter and Intercity Passenger Rail Service,* October 2007
- FTA *Handbook for Transit Safety and Security Certification*, 11/2002
- FTA document *Hazard Analysis Guidelines for Transit Projects*, 01/2000.
- FTA document *Public Transportation System Security and Emergency Preparedness Planning Guide*, 01/2003.
- FTA Circular 5800.1 *Safety and Security Management Guidance for Major Capital Projects*, dated 8/1/07
- Federal Transit Administration manual *Transit Safety Management and Performance Measurement,* FTA Office of Safety and Security, 2011
- ISO 31000 Risk Management Standard

1.0 MANAGEMENT COMMITMENT AND PHILOSOPHY

1.1 Safety and Security Policy Statement

Safety and Security Policy Statement

It is the policy of the California High-Speed Rail Authority (Authority) to perform work on the California High-Speed Train System (CHSTS) in a manner that ensures the safety and security of passengers, employees, contractors, emergency responders, and the public. The application of system safety and security comprises a fundamental hazard and vulnerability management process that incorporates the characteristics of planning, design, construction, testing, operational readiness, and subsequent operation of the high-speed rail system. Safety and security are priority considerations in the planning and execution of all work activities on the CHSTS.

All trains, facilities, systems and operational processes must be designed, constructed, and implemented in a manner that promotes the safety and security of persons and property. The design, construction, testing, and start-up of the CHSTS will comply with applicable safety and security laws, regulations, requirements and railroad industry practices. The Authority will maintain or improve upon the public transit and railroad industry standards for safety and security. Through the Reliability, Availability, Maintainability, and Safety (RAMS) Program a standard of safety will be established that is as safe as or safer than conventional U.S. railroad operations and in conformance with the best practices and standards for safety in the international high-speed rail industry. The design, construction, testing, and start-up of the CHSTS will be accomplished in compliance with this standard.

The Authority is committed to providing a safe and secure travel and work environment. Therefore, safety, accident prevention, and security breach prevention must be incorporated into the performance of every employee task. All Authority, Program Management Team, and contractor personnel, subcontractors and employees are charged with the responsibility for ensuring the safety and security of passengers, employees, contractors, emergency responders, and the public who come in contact with the CHSTS. Each individual and organization is responsible for hazard and vulnerability management, for applying the processes that are designed to ensure safety and security, and for maintaining established safety and security standards, consistent with their position and organizational function. Through a cooperative team effort and the systemic application of safety and security principles, the CHSTS will be designed, constructed, tested, and placed into service in a safe and secure manner.

Jeffrey Morales, CEO
California High-Speed Rail Authority

12-5-12
Date

1.2 Background

The Federal Railroad Administration (FRA) requires that the California High-Speed Rail Authority (Authority) implement safety and security principles and processes throughout the development and operation of the California High-Speed Train System (CHSTS). Absent federal regulations that govern the completion of major capital projects, FRA looks to the Federal Transit Administration (FTA) regulations for guidance. Federal Transit Administration (FTA) regulations found at 49 CFR 633 requires the development of a *Project Management Plan* (PMP) for every major capital transit project. As described in FTA Circular 5800.1 *Safety and Security Management Guidance for Major Capital Projects*, (dated 8/1/07) a *Safety and Security Management Plan* (SSMP) is the element of the PMP that manages project safety and security activities, responsibilities, and verification processes throughout the project life cycle.

This document fulfills the FRA requirement for managing safety and security in the development and operation of the CHSTS.

The SSMP does not carry over into revenue operations, but will lead to development of a System Safety Program Plan and Security and Emergency Preparedness Plan to govern safety and security for the operating system prior to the start of revenue service. The FRA is in the process of promulgating regulations that require the application of a System Safety Program Plan to inter-city passenger railroad operations.

1.3 Purpose of the SSMP

The SSMP formalizes the management principles and strategies for determining safety and security risk acceptance throughout the CHSTS life cycle, from the design phase through the start of revenue service, and is applied to each segment undertaken in turn. The SSMP defines the process for identifying, evaluating, and resolving safety hazards and security vulnerabilities associated with future railroad operations of the System prior to the start of revenue service. This process helps to ensure the achievement of the highest practical level of operational safety and security for the riding public, the employees, and anyone coming into contact with the CHSTS.

The purpose of the SSMP is to define the safety and security activities of the CHSTS and methods for identifying, evaluating, and resolving potential safety hazards and security vulnerabilities. It establishes responsibility and accountability for safety and security during the preliminary engineering, final design, construction, testing, and start-up phases of CHSTS development. Specifically, the SSMP does the following:

- Establishes the Authority‘s commitment and philosophy to achieve the highest practical level of safety and security for the Authority’s staff, Program Management Team (PMT) staff, contractors, emergency responders, and members of the public that come into contact with the CHSTS
- Establishes processes for managing safety and security activities intended to minimize risk of injury and property damage, and to maximize the safety and security for the CHSTS passengers, employees, and the public
- Integrates the safety and security functions and activities throughout the CHSTS and its organizational structure
- Defines the safety and security responsibilities between the Authority and CHSTS design, construction, and start-up teams
- Defines the process for the documentation and certification of safety and security activities
- Evaluates project phases and activities to ensure continued development and advancement of safety and security principles
- Establishes the framework for construction safety and security

1.4 Applicability and Scope of SSMP

The SSMP is applicable to all phases of CHSTS development, from preliminary engineering through final design, construction, testing and the start of revenue service. The SSMP encompasses all equipment, infrastructure, operating and maintenance plans and procedures associated with the CHSTS.

1.4.1 Project Description

The California High-Speed Train System will construct a state-of-the-art, statewide, high-speed performance passenger railroad based on operating practices and designs of existing high-speed rail networks in Europe and Asia which have had extraordinary performance and safety records. The CHSTS will require certification by federal and other regulatory agencies which have indicated they are open to approaches which provide equivalent or better safety than existing rail regulations in the United States. The Authority’s eventual goal is to develop a system of more than 800 route miles that provides high-speed rail service between the major metropolitan centers of the San Francisco Bay Area and

Sacramento in the north, through the Central Valley, to Los Angeles, Anaheim, Irvine and San Diego in the south.

The CHST trains will operate at speeds up to 220 mph within its dedicated or shared-use corridors where the CHSTS has sole use of a track, and up to 125 mph in shared-use conditions where there is joint use of tracks with other passenger trains. There will be no joint use of tracks with freight trains on shared-use tracks. Freight operations, where applicable, will be temporally separated. No hazardous materials will be transported or permitted to be transported by others on Authority dedicated tracks.

The service will use high-speed steel-wheel on steel-rail technology which has been service-proven in Asia and Europe and provides a high level of service in terms of safety, comfort, and reliability. The system will operate on a mostly dedicated, fully grade-separated standard gage track with electric trains powered through the use of an overhead contact system. The right-of-way will make use of tunneling and elevated structures to achieve an ideal alignment and profile. Automotive, animal, other railroad and non-railroad equipment crossings will be accomplished by means of an underpass or overpass.

The system will include an Automatic Train Control (ATC) system based on designs for similar high-speed environments in Europe and Asia, modified only where necessary to meet regulatory requirements and functional and performance needs specific to the CHSTS. The ATC system will cover all functions of a train control system including both safety critical and non-safety critical operations and will incorporate Positive Train Control in compliance with FRA regulations. A hazard detection system will be applied throughout the CHSTS where supported by hazard analysis to alert the operating control center of natural events such as seismic activity, excessive wind speeds, high water levels, and excessive ambient temperature levels that trigger a system response; and other events such as vehicle or rail car intrusion, and trespassers.

1.4.2 Phased Implementation

Although Preliminary Engineering Phase activities will occur simultaneously for the entire system, the Final Design and Construction Phase activities will be developed in phases according to geographic segments, due to the size of the eventual system. The Initial Construction Segment (ICS) has been designated as a point north of Madera to a point north of Bakersfield. Subsequent segments will extend north and south from the ICS.

The Initial Operating Segment (IOS) will encompass several construction segments, with high-speed operations planned between Merced in the north and San Fernando in the south. The IOS will eventually be expanded into what is termed “Bay to Basin”, providing high-speed rail service from the greater San Francisco Bay Area to the greater Los Angeles Basin. The SSMP has been developed with processes that will ensure conformance to system safety goals and requirements throughout the life-cycle of the CHSTS and while various segments are under different development phases simultaneously.

1.4.3 SSMP Scope

This SSMP encompasses the following equipment, facilities, plans, and procedures as they relate to the System.

- System-Wide Elements − includes the passenger vehicles, train control and signaling, voice and data communications, closed-circuit television cameras and recorders, overhead contact system, traction power substations, track, and auxiliary vehicles and equipment
- Fixed Facilities − includes rail stations; pedestrian overpasses and underpasses; highway overpasses and underpasses; aerial and other elevated structures; below-grade structures and tunnels; operations and maintenance facilities including storage yards, shops, and sidings; administrative facilities; and the Central and Regional Control Facilities.
- Safety and Security Plans and Procedures − includes items such as Safety and Security Certification Plan (SSCP), safety and security related Design Criteria, Passenger Train Emergency Preparedness Plan (PTEPP), System Safety Program Plan, and Security and Emergency Preparedness Plan.
- Procedures and Instructions − includes items such as: hazard management, operations and maintenance plans procedures, rulebooks and manuals; and training programs for operating,

maintenance and management employees, employee qualifications, contractor training, and emergency responder training.

1.5 SSMP Goals and Objectives

1.5.1 Goals

The goals of the SSMP are as follows:

- Ensure that the system initiated into revenue service is safe and secure for passengers, employees, emergency response personnel, and the general public through a formal program of safety and security certification
- Ensure that the design, acquisition, construction, fabrication, installation, and testing of critical elements of CHSTS development will be verified for conformance with the established safety and security requirements and validated for achieving an effective level of safety and security
- Ensure that a mechanism is in place for the resolution of any restriction to full safety and security certification
- Establish a Construction Safety and Security Program that provides appropriate safeguards against injuries to employees and the public, damage to property and the environment, as well as minimizes security breaches, during all CHSTS work activities
- Achieve a level of risk that is acceptable to the Authority through a systematic approach to hazard and threat/vulnerabilities management

1.5.2 Objectives

The SSMP goals will be achieved by meeting the following objectives:

- Identifying, evaluating, resolving, and documenting safety hazards and security vulnerabilities at the earliest possible phase of CHSTS development, applying the *Prevention through Design* principle where possible
- Establishing specific safety and security requirements for the CHSTS based on applicable safety and security regulations, codes, standards, guidelines, and recognized best practices both domestically and internationally where applicable
- Verifying that all final drawings, specifications, and contracts issued for the CHSTS conform to the established safety and security requirements
- Implementing CHSTS construction safety and security programs in conformance with established construction safety and security requirements and complying with the California Occupational Safety and Health Administrative safety regulations for construction projects
- Verifying all CHSTS facilities, systems, and equipment have been designed, built, procured, installed, inspected, and tested in accordance with the design criteria and specifications
- Establishing and documenting the qualifications and training programs for all personnel who will operate and maintain the CHSTS in revenue service
- Verifying completion of training of personnel who will respond to emergencies, including CHSTS personnel and emergency responders, on the CHSTS emergency procedures, equipment, and operations
- Conducting and documenting emergency exercises and drills prior to the start of revenue service
- Documenting safety, security, and emergency rules and procedures for CHSTS employees, staff, and contractors in the form of rulebooks, standard operating procedures, emergency operating procedures, and other documents
- Maintaining a process to manage and track open safety and security issues resulting from design deviations, change orders, and non-conformances from inception through closure and acceptance

- Documenting final Safety and Security Certification for the CHSTS segment under consideration by means of a Final Safety and Security Certification Report prior to placing that segment into revenue service
- Ensuring coordination with the Federal Railroad Administration, California Public Utilities Commission, the Transportation Security Administration, the Office of the State Fire Marshal, and other external agencies as applicable

1.6 SSMP Review and Updates

The SSMP will be reviewed at least annually, whenever the Program Management Plan or other reference documents are modified, and following any SSMP audit to ensure the safety and security management program remains current and applicable. If revised, the SSMP will be re-issued to all SSMP recipients. The SSMP will be updated to reflect changes in the CHSTS, the Authority's organizational makeup, or the safety and security management program requirements. The review and update process will be the responsibility of the Authority with the oversight and coordination of the Authority's System Safety Manager.

The Federal Railroad Administration is developing regulations for inter-city passenger rail system safety programs, to be codified under 49 CFR, Part 270. This SSMP is written to be in conformance with proposed regulations for 49 CFR, Part 270 and will support the project management requirements of a System Safety Program Plan.

1.7 SSMP Applicability to Third Parties

The safety and security requirements for third party assets (adjacent infrastructure or operations, shared-use corridors, utility interfaces, etc.) will be developed following the safety and security management program of the applicable third party but in conformance to the processes and requirements of this SSMP. Safety and security certification of third party elements shall conform to the Safety and Security Certification Program requirements of the third party and Section 7.0 of this SSMP.

1.8 System Safety Program Plan and System Security Plan

A System Safety Program Plan (SSPP) will be developed prior to the start of revenue operations. The SSPP will comply with all FRA and other applicable regulatory requirements, and will be appropriate in scope and content to manage the transition the CHSTS safety program from a project to an operating system.

A System Security Program Plan (SSecPP) will also be developed prior to the start of revenue operations. The SSecPP will comply with all Department of Homeland Security (DHS) and other applicable regulatory requirements, and will be appropriate in scope and content to manage the transition the CHSTS security program from a project to an operating system

2.0 INTEGRATION OF SAFETY AND SECURITY INTO THE CHSTS DEVELOPMENT PROCESS

2.1 Safety and Security Activities

This section describes the safety and security activities that have been or will be performed during the major phases of the project. A list of the basic activities and the desired milestone goals are presented in **Table** 2-1. The California High-Speed Train System has four phases:

- Preliminary Engineering
- Final Design
- Construction
- Testing and Startup of Revenue Operations

Although Preliminary Engineering Phase activities will occur simultaneously for the entire system, the Final Design and Construction Phase activities will be developed in phases according to geographic segments, due to the size of the eventual system. The SSMP has been developed with processes that will ensure conformance to system safety goals and requirements throughout the life-cycle of the CHSTS and while various segments are under different development phases simultaneously.

Within each phase of the CHSTS, activities are identified to determine the safety- and security-related certification activities expected to be accomplished at each project milestone. The California High-Speed Rail Authority will apply a detailed and thorough safety and security certification program. The safety and security certification program, as described in Section 7.0 of this SSMP, will ensure that the project achieves all safety and security requirements in design criteria and specifications and that the safety and security contents of the plans, procedures, and training materials are systematically reviewed and revised as required.

Leading up to and through the Preliminary Engineering phase of the project, the safety and security activities encompass the following:

- Develop the SSMP, including a process for achieving safety and security certification, to meet all Federal Railroad Administration (FRA) requirements for a safety and security management plan in a major capital project, in conformance with the Federal Transit Administration's Circular 5800.1 *Safety and Security Management guidance for Major Capital Projects*.
- Develop a list of safety-critical and security-critical elements and items for the CHSTS Preliminary Hazard Analyses.
- Specify safety and security certification requirements, in conformance with the *CHSTS Verification and Validation Management Plan*, in contract documents. Safety and security certification requirements will be part of the scope of work for the design/build contractors during the Final Design and Construction phases of the project.
- Implement a hazard and certification tracking system.
- Perform Preliminary Hazard Analysis (PHA) and a Threat and Vulnerability Assessment (TVA) to identify certifiable elements and hazards/vulnerabilities requiring mitigation. Identify hazard/vulnerability mitigation from the PHA and TVA to be incorporated into preliminary and final designs. Perform additional analysis as required.
- Develop design criteria conformance checklists. The tracking system will be an integrated subset of the Verification and Validation program applied throughout the CHSTS.

Table 2-1 Project Safety and Security Activities Matrix

Task No.	Safety and Security Task	Project Phase			
		Prelim. Engr.	Final Design	Construction	Testing and Startup
1	Develop and update the Safety and Security Management Plan (SSMP)	√	⇒	⇒	⇒
2	Identify Certifiable Elements and Items	√	⇒	⇒	⇒
3	Specify Safety and Security Certification Requirements into Contract Documents	√	⇒	⇒	⇒
4	Implement Certification Tracking System	√	⇒	⇒	⇒
5	Conduct Preliminary Hazard Analysis (PHA) and Threat and Vulnerability Assessment (TVA) and Resolve Unacceptable Hazards and Vulnerabilities	√	⇒	⇒	⇒
6	Develop Design Criteria Conformance Checklists	√	⇒		
7	Conduct Independent Safety and Security Audits		√	⇒	⇒
8	Verify Design Criteria Conformance Checklists and Issue Certificates		√	⇒	
9	Develop Construction Specification Conformance Checklists		√	⇒	
10	Develop Safety-Related Testing Conformance Checklists			√	⇒
11	Verify Specification Conformance Checklists			√	⇒
12	Verify Safety-Related Testing Conformance Checklists				√
13	Verify Operations and Maintenance Manuals Conformance			√	⇒
14	Complete Contractor Training			√	⇒
15	Complete Rules and Procedures and Issue Certificates			√	⇒
16	Complete Operations Training and Issue Certificates				√
17	Complete Emergency Services Training				√
18	Complete Emergency Response Exercises				√
19	Issue Phase Safety/Security Certificate of Conformance				√
20	Issue Final Safety/Security Certification Report				√

Note: √ = Task activity initiated
⇒ = Task activity updated

2.2 Procedures and Resources

2.2.1 Procedures

A *CHSTS Project Management Plan* (PMP) for the system has been prepared. The PMP establishes the framework for managing and administering all activities related to implementation of the system and provides guidance for the coordination of activities. The PMP identifies that the PMT is responsible for

developing the basic design requirements of the high-speed rail system, ensuring that common approaches for the environmental and outreach work are used through the entire alignment, preparing and helping execute bid and procurement processes for design, construction, maintenance, and operations, and managing the work of or coordinating with a variety of other consultants to the Authority, notably the Regional Consultants (RC).

A major component of the PMP is this *Safety and Security Management Plan*, describing processes for identifying and managing hazards and vulnerabilities associated with the CHSTS. It is the responsibility of the Authority to ensure that the management of identified safety hazards and security threats and vulnerabilities is effective and integrated throughout the design, construction, testing, and startup phases of the CHSTS.

The verification and validation process will be applied throughout the CHSTS for the purpose of tracking and verifying that critical elements are incorporated into all project phases. Critical elements include safety-critical and security-critical elements as identified though the hazard management processes identified in this SSMP.

2.2.2 Resources

The Chief Executive Officer authorizes the SSMP, ensuring that it is applied throughout the CHSTS. The Risk Manager administers and oversees the implementation of the SSMP. The Authority will provide additional safety and security management resources for executing the system safety and security activities during the Preliminary Engineering phase. Further resources and responsibilities will be identified as the system progresses into later phases, culminating in startup and commissioning.

The budget and schedule for implementation of the SSMP is revised each year and is held with the Risk Manager. This assures that the requirements of the SSMP are executed by the Authority, supported by the PMT, during the Preliminary Engineering phase and in subsequent phases of the project. This includes, but is not limited to, the performance of safety analyses and security assessments at the appropriate phases of the project; implementation of a Safety and Security Certification Program beginning at Preliminary Engineering and continuing through each subsequent phase of the project; a process to ensure that safety issues and security concerns are addressed and tracked to resolution; and construction safety oversight activities as appropriate to the Construction phases and contracts under way at the time.

2.3 Interfacing with Management

The California High-Speed Rail Authority Chief Executive Officer, through the Authority Director of Risk Management and Project Controls, has the ultimate decision-making authority for safety and security issues and is responsible for communication of safety and security issues to the Authority Board of Directors. The Authority Director of Risk Management and Project Controls will oversee the overall implementation of the safety and security program and will report the progress and challenges in its implementation to the Safety and Security Program Committee. The Safety and Security Program Committee will communicate the safety and security issues to the Authority executive management through reports to the Safety and Security Executive Committee.

Successful implementation of the SSMP will also require significant interaction between various members of the Authority, the Program Management Team, Regional Consultants, Engineering/Construction Managers, and Emergency Response Agencies. These interactions will occur during regularly scheduled meetings of the Safety and Security Program Committee and Safety and Security Executive Committee that focus on the safety and security aspects of the system.

3.0 SAFETY AND SECURITY RESPONSIBILITIES

3.1 Roles and Responsibilities

The California High-Speed Rail Authority (Authority) is responsible for developing a high-speed train system in California in a safe and secure manner, ensuring that all trains, facilities, systems and operational processes are designed, constructed, and implemented in a manner that promotes the safety

and security of persons and property. The Authority has the ultimate authority and responsibility for the implementation of the *Safety and Security Management Plan* (SSMP) for this system. The Authority is tasked to prepare a plan and design for the system, conduct environmental studies and obtain necessary permits, and undertake the construction and operation of a high-speed train passenger network in California.

The Authority Safety and Security Manager, under the direction of the Authority Director of Risk Management and Project Controls, administers and oversees the implementation and activities of the Safety and Security Program. The Authority's primary vehicle for oversight of the safety and security activities is a two-tiered organization of safety and security committees (explained in detail in Section 3.3).

The Federal Railroad Administration (FRA) is the lead agency for the Federal Environmental Impact Statement. The FRA is also the primary regulatory agency responsible for approving and certifying the system safety and security aspects of the CHSTS. At the state level, the California Office of the State Fire Marshal has regulatory authority over the fire and life safety aspects of the occupied structures, including right-of-way access/egress facilities

The Authority has contracted with Parsons Brinckerhoff (PB) as the Program Management Team (PMT), and five Regional Consultant (RC) teams to conduct the preliminary engineering on specific segments of the line and provide overall Program Management for the CHSTS.

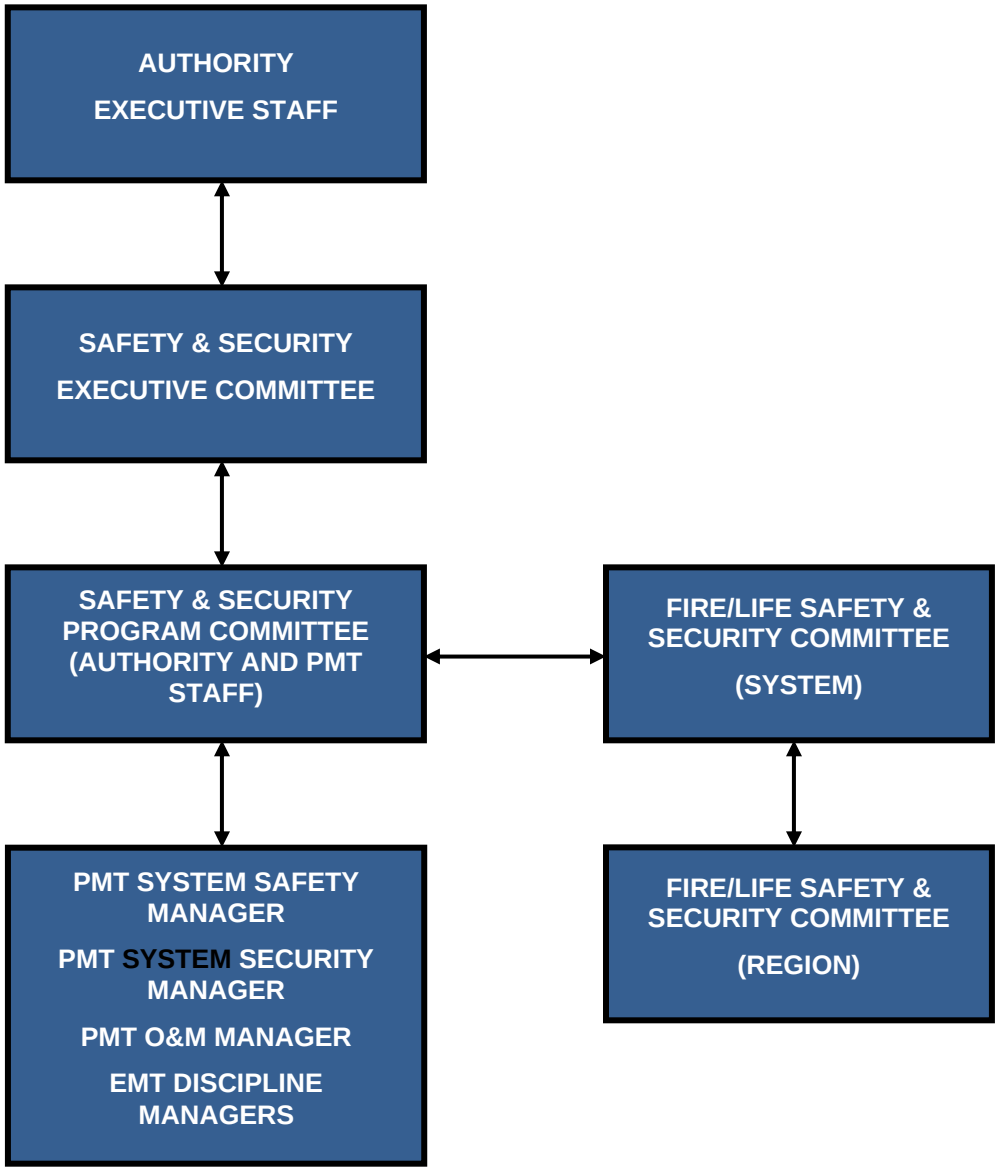
The PMT is responsible for the management of the preliminary design of the high-speed train system, including ensuring that system safety and security is applied consistently and effectively for the entire CHSTS alignment and across all phases of the project.

The PMT Safety and Security Managers will support the Authority Safety and Security Manager in the application of safety and security in all aspects and phases of the project coordinating with the Program Deputy Directors, Discipline Managers, and Regional Managers. This support will ensure that other individual project staff members perform in accordance with the SSMP in establishing and overseeing the safety and security management tasks. The PMT's primary vehicle for input to and support of the safety and security activities is the Safety and Security Program Committee (explained in detail in Section 3.3.2).

Staff members assigned to the CHSTS by the Authority, PMT, contractors, consultants, emergency response agencies, FRA and CPUC are responsible for ensuring that the design, construction, installation, and testing of all safety-critical and security-critical system elements of the system are evaluated for conformance with the safety and security requirements and verified for operational readiness before completing each phase of the project.

Refer to Figure 3-1 for the CHSTS organizational chart for safety and security activities. This SSMP shall be updated to reflect any significant changes in the organizational structure or definition of responsibilities with respect to safety and security in the CHSTS.

Figure 3-1 CHSTS Organization for Safety and Security Activities



3.2 Authority Organization

The Authority has a nine-member policy board and a core staff, supported by contract with private consulting firms (the Program Management Team, Regional Consultants and other specialty firms) to carry out the project's system safety and security programs, environmental studies, project planning and engineering work under the supervision and guidance of Authority staff. The Authority's Director of Risk Management and Project Controls is responsible for safety and security activities, reporting directly to the Chief Executive Officer.

The project organization will remain in place throughout the CHSTS development process; however, the composition of the project organization may be revised to respond appropriately to the changing project needs as the project proceeds through from the preliminary engineering phase through to the start of revenue service. The Authority project organization during the initial project phases comprises the Authority and Program Management Team staff supplemented by Regional Consultant staff. In each

phase, the Authority will use the assistance of the PMT to manage project-related activities, as well as further assistance from professional engineering and other project management consulting firms.

The current California High-Speed Rail Authority organization is shown in Appendix A.

3.2.1 Authority Chief Executive Officer

The Authority Chief Executive Officer oversees and directs the management of all Authority staff and the Program Management Team. The day-to-day management of the development activities for the California High-Speed Train System is the functional responsibility of the Authority Program Director under the direction of the Authority Chief Executive Officer. The Authority Chief Executive Officer ensures that Authority resources are allocated to meet the SSMP goals and objectives, and is ultimately responsible for execution of the *Safety and Security Management Plan* through the Authority Director of Risk Management and Project Controls and the Authority Safety and Security Manager. The Authority Chief Executive Officer chairs the Safety and Security Executive Committee and reports to the Authority Board of Directors.

3.2.2 Authority Director of Risk Management and Project Controls

The Authority Director of Risk Management and Project Controls reports directly to the Authority Chief Executive Officer and is responsible for identifying, managing and tracking risks and risk mitigation/contingencies, and all responsibilities related to safety and security management on the project, His duties also include maintaining the risk management tool and documentation information, leading risk identification sessions for the project, monitoring prime contractor risk management efforts, and participating in risk management activities for risks that cross project boundaries or are beyond the project's control. He chairs the Safety and Security Program Committee and directs active management of all safety and security efforts for the project and reports activities from the Safety and Security Program Committee to the Safety and Security Executive Committee.

3.2.3 Authority Safety and Security Manager

The Authority Safety and Security Manager is responsible for the management of all safety and security activities associated with the development and implementation of the CHSTS. The Authority Safety and Security Manager is a member of the Safety and Security Executive Committee and Safety and Security Program Committee, and advises the Authority on policy decisions with regard to safety and security. The Authority Safety and Security Manager reports directly to the Authority Director of Risk Management and Project Controls and coordinates safety activities with the PMT Safety and Security Managers.

The Authority Safety and Security Manager has the authority and responsibility for, but is not limited to the following:

- Ensuring that the SSMP requirements and processes are being implemented and that SSMP goals and objectives are being achieved
- Oversight of the PMT safety and security activities
- Developing corrective action plans (CAPs) that result from accident/incident investigations, hazard analyses, certification of Certifiable Items List (CIL), and safety and security reviews and audits; and tracking corrective actions through closeout to ensure that all identified deficiencies are adequately mitigated or controlled
- Providing oversight for the Contractors' job site safety and programs
- Reviewing and supporting Authority decision for Contractor's safety submittals
- Investigating accidents and incidents on behalf of the Authority
- Reporting unacceptable hazardous conditions to executive management as soon as possible
- Fulfill the role of Chair for the Fire and Life-Safety and Security Statewide Committees

3.3 Program Management Team Organization

3.3.1 PMT System Safety Manager

The PMT System Safety Manager will support the Authority Safety and Security Manager in the implementation and completion of all safety activities associated with the development of the CHSTS. The PMT System Safety Manager will coordinate safety activities with the PMT System Security Manager, PMT Discipline Managers, PMT Construction Safety Officers, and sit on the Safety and Security Program Committee, Safety and Security Executive Committee, and Fire and Life-Safety and Security Committees as requested. The PMT System Safety Manager's role on the Committees is to ensure that safety and security are not compromised by other priorities of the design and construction teams.

The PMT System Safety Manager has the responsibility for, but is not limited to, the following:

- Performing hazard management of CHSTS elements and design criteria to determine any potential hazards that may be created by system development, expansion or modification, and supporting the development of mitigating and controlling factors to address such hazards
- Participating in the project design reviews, including overseeing and administering formal safety and security certification programs
- Working with PMT engineering, operations and maintenance staff to ensure that the system is being designed to safety and security criteria
- Fulfilling the role of Secretary for the Safety and Security Program Committee, and the Fire and Life-Safety and Security Statewide and Regional Committees
- Supporting Authority outreach efforts to local, regional and State emergency response agencies
- Performing other safety-related activities as requested by the Authority

3.3.2 PMT System Security Manager

The PMT System Security Manager will support the Authority Safety and Security Manager in the implementation and completion of all security activities associated with the development of the CHSTS. The PMT System Security Manager will coordinate security activities with the PMT System Safety Manager, PMT Discipline Managers, and sit on the Safety and Security Program Committee, Safety and Security Executive Committee, and Fire and Life-Safety and Security Committees as requested. The PMT Security Manager's role on the Committees is to ensure that security requirements are not compromised by other priorities of the design and construction teams.

The PMT System Security Manager has the responsibility for, but is not limited to, the following:

- Performing threat and vulnerability assessments of CHSTS operating environments and design criteria to determine any potential vulnerabilities that may be created by system development, expansion or modification, and supporting the development of mitigating and controlling factors to address such vulnerabilities
- Participating in the project design reviews, including overseeing and administering formal safety and security certification programs
- Working with PMT engineering, operations and maintenance staff to ensure that the system is being designed to safety and security criteria
- Supporting Authority outreach efforts to local, regional and State emergency response agencies and law enforcement agencies
- Performing other security-related activities as requested by the Authority

3.3.3 PMT Construction Safety Officer

The PMT Construction Safety Officer will support the Authority Construction Manager and Safety and Security Manager in the implementation and completion of all safety activities associated with the construction of the CHSTS.

The PMT Construction Safety Officer has the responsibility for, but is not limited to, the following:

- Oversight of the Project Construction Management (PCM) teams for safety and security activities
- Field audits and inspections of construction activities on behalf of the Authority
- Accident investigation and follow-up
- Development of field safety rules and procedures for Authority and PMT staff
- Training to support Authority and PMT field safety rules and procedures
- Safety Management System data collection, analysis, and documentation

3.3.4 Other Managers

The managers of the following disciplines will be responsible for implementing the SSMP requirements and process in their respective areas, participating in the SSPC and for supporting the Authority Safety and Security Manager as required:

- Engineering, including Infrastructure and Systems
- Operation and Maintenance
- Rolling Stock
- Integration and Regulatory Approvals
- Project Risk
- Contracts and Procurement
- Verification and Validation

3.4 Committee Structure

Chapter 2 of the PMP describes the function of various project committees. In addition, safety and security committees listed below will be established to facilitate review of issues and to provide a forum for discussion and resolution.

3.4.1 Safety and Security Executive Committee

The Safety and Security Executive Committee (SSEC) and its members will ensure that the CHSTS is designed, built, and implemented in a safe and secure manner. The SSEC will achieve this goal by providing oversight of the application of the SSMP through all phases of the CHSTS development and to act as a conduit to informing and assuring Authority executive management of safety and security issues.

The Safety and Security Executive Committee will address safety and security issues that are Authority policy considerations, require Authority approval, require Authority direction for resolution of a dispute, or constitute final acceptance of safety and security certification.

The duties and responsibilities of the Safety and Security Executive Committee are as follows:

- Provide guidance to and approval of policy decisions with respect to safety and security
- Provide a forum for safety and security discussions among Authority Executive Management, discipline leads, and PMT Management
- Authorize the establishment of the Safety and Security Program Committee (SSPC)
- Review and approve regular reports of safety and security activities from the SSPC
- Resolve safety and security issues that cannot be resolved at the SSPC level
- Review and approve a final Safety and Security Certification Report prior to the startup of revenue operations

The Safety and Security Executive Committee comprises the following persons:

- Authority Chief Executive Officer (Chairperson)
- Authority Director of Risk Management and Project Controls
- Authority Risk Manager
- Authority Regional Directors
- Authority Chief Operating Officer
- Authority Chief Engineer
- Authority Chief Counsel
- Authority Construction Manager
- Authority Environmental Manager
- PMT Program Director (advisory role)
- PMT System Safety Manager (Secretary - advisory role)
- PMT System Security Manager (advisory role)

The Chairperson of the SSEC is the Authority Chief Executive Officer or a designated Authority executive management representative. If a designated member of the SSEC is unable to attend a SSEC meeting, they must assign an appropriate representative.

The SSEC Charter, Technical Memorandum 500.02, can be found in Appendix C of this SSMP.

3.4.2 Safety and Security Program Committee

Working at the project delivery level, the Safety and Security Program Committee (SSPC) will ensure that the CHSTS is designed, built, and implemented in a safe and secure manner. The SSPC will achieve this goal by providing oversight of the application of the SSMP through all phases of the CHSTS development and to act as a conduit to informing and assuring Authority executive management (through the SSEC) of safety and security issues affecting the project.

The SSPC will address safety and security issues which are directed to it by the SSEC, require project delivery level resolution, require elevation to the SSEC for Authority direction for resolution, or constitute preliminary review and approval of Safety and Security Certification.

The duties and responsibilities of the Safety and Security Program Committee are as follows:

- Approve the initial version of the SSMP and subsequent updates
- Oversee the application of the SSMP through all CHSTS development phases
- Tracking of identified hazards or vulnerabilities listed on Certified Elements and Hazards List using the V&V Requirements Management Tool database
- Provide regular reports of safety and security activities to the SSEC
- Forward to the SSEC for resolution any safety and security issues that cannot be resolved at the SSPC level
- Review and approve safety and security certification Certificates of Conformance and a Final Certification Verification Report for each project phase
- Forward a final Safety and Security Certification Report to SSEC for Authority approval prior to the startup of revenue service
- Provide a forum for safety and security discussions among PMT staff members and a conduit for safety and security issues to the Authority through the SSEC

The Safety and Security Project Committee is made up of the following persons:

- Authority Director of Risk Management and Project Controls (Committee Chairperson)
- Authority Risk Manager

- PMT System Safety Manager (Committee Secretary)
- PMT System Security Manager
- PMT Program Director
- PMT O&M Manager
- EMT Discipline Managers
- PMT Verification & Validation Manager
- PMT Contracts Manager
- PMT Project Risk Manager
- PMT RAMS Manager
- PMT Environmental Planning Manager

If a designated member of the SSPC is unable to attend a SSPC meeting, they must assign an appropriate representative.

The SSPC Charter, Technical Memorandum 500.03, can be found in Appendix D of this SSMP.

3.4.3 Fire and Life Safety and Security Committees (FLSSC)

The Fire and Life Safety and Security Committees (FLSSC) will be composed of representatives from fire, police and local building code agencies assigned to two levels of standing committees: a Statewide FLSSC and several regional FLSSC working on a local level. The CHSTS will form the FLSSC during the Preliminary Engineering phase of the project. The purpose of the FLSSC will be to review issues that are critical to fire and life safety and security, to acquire input and concurrence from the state and local authorities having jurisdiction over the proposed designs to meet code requirements, and to ensure compliance with state and local fire code standards or fire/life safety hazard mitigation measures during the design phase. As the project moves into the Testing and Startup Phase the FLSSC will review operating plans and procedures, results of after-action reviews following major emergency response incidents or exercises, and training programs for content appropriateness and effectiveness.

The single statewide FLSSC will focus on systemic, high-level, fire/life safety and security issues, including federal and state codes or requirements impacting the regional efforts. A goal of the system FLSSCs is to obtain concurrence from federal and state authorities with respect to fire and life safety and security concerns. The system FLSSC will include a representative from each regional FLSSC as well as representatives from state and federal agencies such as the California Office of the State Fire Marshal, California Highway Patrol, California Office of Emergency Services, CPUC, FRA, and DHS. The system FLSSC will be chaired by the Authority's Risk Manager. Meetings will be held regularly in Sacramento with agendas, minutes, and other support materials supplied by the committee co-chairs. Minutes and action items from the meetings will be conveyed to the regional FLSSCs and to the Safety and Security Program Committee for their consideration

Regional FLSSCs will focus on the CHSTS characteristics specific to their corridor segments (type/length of underground and elevated structures, access methods, terminals, etc.) to provide input with respect to local building codes or requirements that are in line with the emergency response characteristics and capabilities of the local agencies. A goal of the regional FLSSC is to obtain concurrence from local authorities with respect to the proposed designs and the code requirements of the state and federal authorities having jurisdiction. The regional FLSSC will be composed of appropriate representatives (e.g., Fire Marshal, Police Chief) from local emergency response agencies (fire, police, EMT) and will be chaired by the PMT System Safety and Security Managers or designees. Meetings will be held regularly at a location local to the regional corridor, with agendas, minutes, and other support materials supplied by the committee co-chairs. Minutes and action items from the meetings will be conveyed to the system FLSSC and to the Safety and Security Program Committee for their consideration. One representative from each regional FLSSC will be asked to participate in the system FLSSC. Consistent membership is critical to success. Each regional representative must be the same representative attending to System FLSSC matters and reporting results to their specific Regional Committee.

The FLSSC Charter, Technical Memorandum 500.04, can be found in Appendix E of this SSMP.

3.4.4 Program Change Control Board

Change control for the CHSTS will be in conformance with *PC2.04 Program Change Control Procedure*. The procedure includes a Change Control Board made up of Authority, PMT, and PMO representatives.

3.4.5 Rail Activation Committee (RAC)

The Rail Activation Committee (RAC) will coordinate planning and process development efforts for the operational testing of the system and eventual startup of revenue service. The RAC will be multi-disciplinary in scope and will be established during the latter stages of the Construction Phase.

3.4.6 System Integration Testing Committee (SITC)

The System Integration Testing Committee (SITC) will coordinate the development of an integrated testing program. The SITC will plan for the effective and efficient testing of subsystems, and then the overall system, including ensuring that as testing progresses mitigations are taken to ensure the safety of the tests. The maturity of the various subsystems will be taken into account prior to full development and assurance that the systems are proven safe. The SITC will be multi-disciplinary in scope and will be established during the latter stages of the Construction Phase.

3.5 Safety and Security Responsibilities Matrix

The requirements, authority, and activities for safety and security will be integrated into the overall project management. At each stage of project advancement, there will be a process in place to ensure that the appropriate parties are aware of their safety and security responsibility associated with the project activity. The Safety and Security Responsibility Matrix (Table 3-1) lists the activities to be performed and assigns the responsibilities from the Preliminary Engineering phase through system Start-up phase.

Table 3-1 Safety and Security Responsibilities Matrix

Key Safety and Security Certification Steps	Preliminary Engineering Phase					Final Design Engineering Phase					Construction Phase					Testing/Startup Phase				
	AUT	S/S	PMT	CMT	DBC	AUT	S/S	PMT	CMT	DBC	AUT	S/S	PMT	CMT	DBC	AUT	S/S	PMT	CMT	OMC
Develop/Update Certifiable Elements and Hazards Log	A	P	S	-	-	-	A	S	S	P	-	A	S	S	P	-	A	S	S	P
Hazard and Vulnerability Analyses	A	P	S	-	-	A	P	S	S	S	A	P	S	S	S	A	P	S	S	S
Develop S/S Design Criteria	A	P	S	-	-	A	P	S	S	S	A	P	S	S	S	A	P	S	S	S
Develop V&V Certifiable Items Lists	A	P	S	-	-	-	A	S	S	P	-	A	S	S	P	-	A	S	S	P
Verification of S/S Certifiable Items Lists	A	S	P	-	-	-	A	S	S	P	-	A	S	S	P	-	A	S	S	P
Issue Phase Certificates of Conformance	A	P	S	-	-	-	A	A	S	P	-	A	A	S	P	-	A	A	S	P
Approve Phase Certs. Of Conformance	P	S	S	-	-	P	S	S	-	-	P	S	S	-	-	P	S	S	-	-

Abbreviations: AUT = Authority Safety & Security; S/S = PMT Safety & Security; PMT = Program Mgmt. Team; DBC = Design/Build Contractors; OMC = Operations & Maintenance Contractors; CMT = Construction Mgmt. Team; PE = Preliminary engineering Phase; FD = Final Design Phase; CN = Construction Phase; TS = Testing & Startup Phase

Responsibilities: P = Primary S = Supporting A = Audit - = None

4.0 HAZARD MANAGEMENT

4.1 Overview

A hazard is an intentional or unintentional condition or circumstance that has the potential to cause injury, illness, death, damage or loss of equipment or property, or severe environmental damage. Safety hazards (unintentional) or security hazards (intentional) both require management to identify and reduce the risk to the Authority

A risk assessment process for the management of safety and security hazards will be used for the CHSTS. The purpose of the process is as follows:

- Identify and evaluate the effects of hazardous conditions on passengers, CHSTS personnel, CHSTS infrastructure and equipment in order to apply mitigation measures that allow the Authority to achieve an acceptable level of risk.
- Define and evaluate mitigation measures to eliminate or control the identified safety and security hazards.
- Document the development and incorporation of safety and security measures on a Certifiable Elements and Hazards Log (CEHL) during System development and implementation, demonstrating how an acceptable level of safety and security is to be achieved.

The development of the safety hazard analyses and security risk assessments will be coordinated with the appropriate engineering disciplines for the identification of applicable hazards and recommended control measures. Supporting documentation will be submitted to the SSPC for review. The SSPC will elevate the reports to the Authority, through the SSEC, as appropriate to the processes described in Section 3.4.

Hazard management processes will be applied to the development of the System throughout the entire System life cycle. As the System enters Final Design, the design/build contractors will review and update the CEHL for the geographic section under consideration, and work with the Authority to perform or support other analyses as warranted by local or site-specific conditions or designs. Any deviations to the Design Criteria will follow the procedures outlined in section 5.4. Other hazards may be identified during the normal course of work on the development of the CHSTS, including such activities as design reviews, construction inspection and testing, and start-up and integrated testing. Additional hazards or vulnerabilities identified during these activities will also require a hazard analysis or vulnerability assessment to be performed.

The SSPC will be responsible for reviewing and approving all hazard analyses and vulnerability assessments to ensure that significant safety hazards and security threats and vulnerabilities are identified and that the proposed countermeasures adequately resolve the issues. The SSPC will monitor the status of the identified hazards and vulnerabilities from initial identification through final resolution and closure in conformance with the V&V process and by utilizing reports from the V&V Requirements Management Tool database. Sensitive security issues will be tracked on a separate log per the CHSTS SSI Program.

4.2 Risk-Based Safety Hazard Management

Risk-based safety hazard management addresses hazards to the system based upon the amount of risk, both the severity and frequency, posed by the hazard. Hazards that represent higher levels of risk will receive higher levels of resources and analysis.

The risk-based hazard management process is the overall iterative process that comprises:

- System definition
- Hazard identification
- Risk analysis

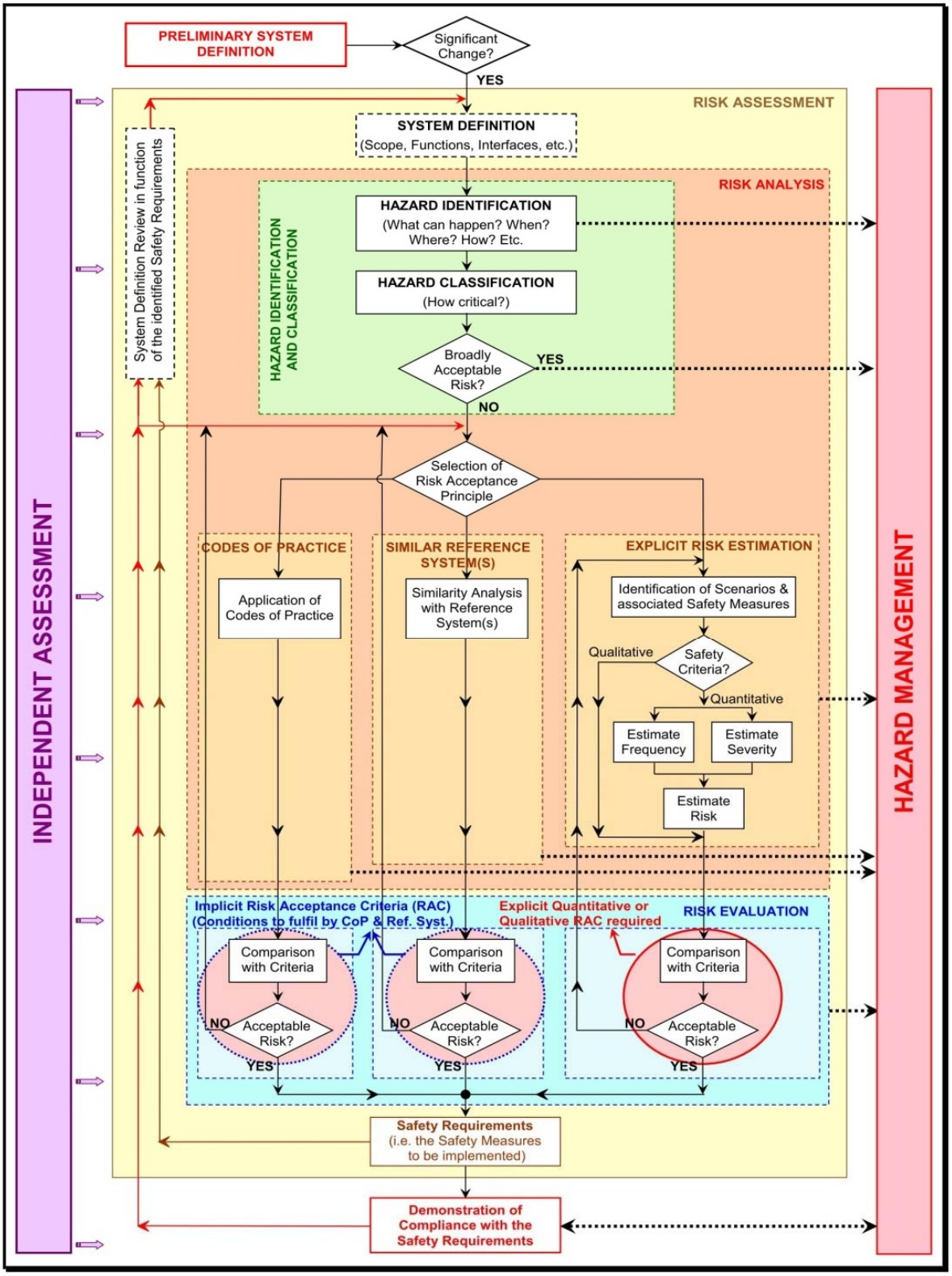
- Accepting residual risk after the application of measures of mitigation
- Verification and validation of implemented hazard management elements

Risk-based hazard management shall be the responsibility of the Authority or its designated representative, but subject to review by an Independent Safety Assessment body (ISA). Risk-based hazard management will begin at the system level and flow-down to sub-system or site-specific levels as appropriate to capture relevant information and sufficient detail to provide appropriate input to the hazard analysis process.

4.2.1 Application of Risk-Based Hazard Management –Common Safety Method

Risk-based hazard management shall be applied to a new system or sub-system and to significant safety-related technical, operational, or organizational changes to the CHSTS using a process called Common Safety Method (CSM). The CSM applied to the CHSTS is based upon the process identified in the European Commission Regulation No. 352/2009 and described in the UK Office of Rail Regulation's (ORR) *Guidance on the Application of the Common Safety Method (CSM) on Risk Evaluation and Assessment*, December 2012. The main phases of the CSM process are illustrated in Figure 4-1. Note that the significant change referenced in Figure 4-1 also implies application to new systems or sub-systems.

Figure 4-1 The Common Safety Method Process



To determine the significance of a new system, sub-system, or change, the following six criteria should be examined:

- Failure consequence: most reasonable credible mishap scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system
- Novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organization implementing the change
- Complexity of the change
- Monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions
- Reversibility: the inability to revert to the system before the change
- Additionality: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant

Guidance on determining significance can be found in SSMP Appendix G *ORR Guidance on the Application of the CSM, Annex 1, December 2012*.

Technical changes are changes to structural and functional railway sub-systems. Technical changes should also be reviewed to determine whether they introduce changes to the operation of the railway sub-system under consideration.

Examples of operational changes include the following:

- Changes to the operation of the CHSTS as a whole
- Changes to the operation of a structural CHSTS sub-system
- Changes to the operating rules of the CHSTS

Changes to the operation of a CHSTS sub-system may be caused by technical changes to that sub-system. In this case, the technical change and its effect on the operation of the CHSTS sub-system, and any changes to the operation or operating rules of the CHSTS system, should be assessed together. For example, a change in the wayside signaling may result in increased line capacity. The technical change (new wayside signals) should be assessed together with the operational change (added trains to the line). However, changes to the operation or operating rules of the CHSTS system can be introduced without a related technical change. The CSM should be used to assess whether these safety-related changes are significant or not. If they are significant, the CSM should be applied to these changes.

Technical changes to a sub-system can also introduce changes to the operating rules of the railway system. Changes to the operating rules of the CHSTS should be considered together with the technical change, the change to the operation of the affected CHSTS sub-system, and any change to the operation of the CHSTS as a whole.

Organizational changes are changes to the organization of an actor or entity within the CHSTS which could impact on the safety of the CHSTS. The “actor” could be any organization (Authority, contractor, sub-contractor, etc.) that directly affects the safety of the CHSTS. Guidance on organizational changes can be found in SSMP Appendix H *ORR Guidance on the Application of the CSM, Annex 4, December 2012*.

4.2.2 System Definition

The CSM process starts with the system definition. This provides the key details of the new system or the system that is being changed - its purpose, functions, interfaces and the existing safety measures that apply to it. In most cases, the hazards which need to be analyzed will exist at the boundary of the system with its environment. The definition is not static and during iterations of the risk management process, it should be reviewed and updated with the additional safety requirements that are identified by the risk

analysis. It, therefore, describes the condition (or expected condition) of the system before the change, during the change, and after the change.

The system definition shall address at least the following issues:

- System objective, (e.g., intended purpose)
- System functions and elements, where relevant (e.g., human, technical and operational elements)
- System boundary including other interacting systems
- Physical (i.e., interacting systems) and functional (i.e., functional input and output) interfaces
- System environment (e.g., energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use)
- Existing mitigation measures and definition of the safety requirements identified by the hazard risk assessment process
- Assumptions that shall determine the limits for the hazard risk assessment

The system definition needs to cover not only normal mode of operations but also degraded or emergency mode.

Consideration of interfaces should not be restricted to physical parameters, such as interfaces between wheel and rail. It should include human interfaces, for example the user-machine interface between the locomotive engineer and displays in the cabs of rail vehicles. It should also include interfaces with non-railway installations and organizations, for example, the interface with underground utilities.

Operational procedures and rules, and staff competence should be considered as part of the system environment in addition to the more usual issues such as weather, electromagnetic interference, local conditions such as lighting levels, etc. The system definition is complete and sufficient if it describes the system elements, boundaries and interfaces, as well as what the system does.

The description can effectively serve as a model of the system and should cover structural issues (how the system is constructed or made up) and operational issues (what it does, and how it behaves normally and in failure modes). The existing safety measures, which may change as the risk assessment process progresses, can be added after the structural and operational parts of the model are complete.

The Hazard Assessor may not know all the environmental or operational conditions in which the altered or new system will operate. In these circumstances, they should make assumptions on the basis of the intended or most likely environment. These assumptions will determine the initial limits of use of the system and should be recorded. When the system is put into use, the Hazard Assessor (who may be different to the original proposer) should review the assumptions and analyze any differences with the intended environmental and operational conditions.

4.2.3 Hazard Identification and Classification

The Authority shall systematically identify, using wide-ranging expertise from a competent team, all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate, and its interfaces. Scope of hazards shall be limited to those hazards that directly or indirectly affect the safety of passengers, employees, rolling stock, and facilities of the CHSTS. All identified hazards shall be registered in the CEHL.

The purpose of the hazard identification is to identify all reasonably foreseeable hazards which are then analyzed further in the next steps.

The hazard identification should be systematic and structured, which means taking into account factors such as the following:

- The boundary of the system and its interactions with the environment
- The system's modes of operation (i.e., normal/degraded/emergency)

- The system life cycle including maintenance
- The circumstances of operation (e.g., proximity to freight-only line, tunnel, bridge, etc.)
- Human factors
- Environmental conditions
- Relevant and foreseeable system failure modes

Relevant tools for hazard identification include structured brainstorming, checklists, task analysis, operations analysis, preliminary hazard analysis, and failure modes and effects analysis. Whichever technique is used, it is important to have the right mixture of experience and competence while maintaining impartiality and objectivity. Correct hazard identification will underpin the whole risk assessment process and give assurance that the risks will be managed in the project.

Preliminary Hazard Analysis (PHA) shall be performed in order to identify an initial risk index for hazard classification and to form a basis for risk acceptance. Development of the PHA involves identifying the severity of consequence and frequency of occurrence before the application of mitigation measures, using the risk estimation process and risk acceptance criteria identified in Section 4.2.5. The PHA form shall be completed in accordance with the PHA process identified in SSMP Appendix I.

Development of the PHA will allow classification of the hazard as broadly acceptable or not. Based on expert judgment, hazards associated with a broadly acceptable risk need not be analyzed further but shall be registered in the CEHL. In this context, 'broadly acceptable' applies to those hazards where the risk is essentially insignificant or negligible. Their acceptable classification shall be justified in order to allow acceptance by the Authority.

The level of detail of the hazard identification depends on the system that is being assessed and needs to be sufficient to ensure that relevant safety measures can be identified. If it can be successfully demonstrated that a hazard can be controlled by application of one of the three risk assessment principles identified in the CSM, following high-level hazard identification, then no further hazard identification is necessary. If it is not possible to have sufficient confidence at this stage, then further analysis of the causes of these high level hazards is undertaken to identify relevant measures to control the risks arising. The risk assessment process continues until it can be shown that the overall system risk is controlled by one or more of the risk assessment principles.

Hazard identification is still necessary for those systems/sub-systems/changes where the hazards are controlled by the application of codes of practice or by comparison to reference systems. Hazard identification in these cases will serve to check that all the identified hazards are being controlled by relevant codes of practice or by adopting the safety measures for an appropriate in-use system. This will also support mutual recognition and transparency. The hazard identification can then be limited to verification of the relevance of the codes of practice or reference systems, if these completely control the hazards, and identification of any deviations from them. If there are no deviations, the hazard identification may be considered complete.

During the hazard identification, mitigation measures may be identified as well. Potential mitigation measures shall be registered in the CEHL.

The hazard identification only needs to be carried out at a level of detail necessary to identify frequency and severity of the hazard, plus potential mitigations. Development of sub-system analysis may be necessary until a sufficient level of detail is reached for the identification of hazards.

4.2.4 Risk Analysis

The risk acceptability of the system under analysis shall be established by following this hierarchy of CSM Risk Acceptance Principles:

1. The application of codes of practice (Section 4.2.4.1)
2. A comparison with reference systems (Section 4.2.4.2)

3. Explicit risk estimation (Section 4.2.4.3)

More than one of these risk acceptance principles may be applied in concert. The Hazard Assessor shall demonstrate in the risk evaluation that the selected risk acceptance principle is adequately applied. The Hazard Assessor shall also ensure that the selected risk acceptance principles are used consistently. The Authority is ultimately responsible for approving the risk evaluation efforts of the Hazard Assessor and accepting the residual risk associated with the identified hazard or vulnerability.

Whenever a code of practice or a reference system is used to control the risk, the hazard identification must also include the following:

- The verification of the relevance of the code of practices or of the reference system
- The identification of the deviations from the code of practices or from the reference system

The application of CSM Risk Acceptance Principles shall identify possible mitigation measures that make the risk(s) of the system under assessment acceptable. Among these mitigation measures, the ones selected to control the risk(s) shall become the safety requirements to be fulfilled by the system. Compliance with these safety requirements shall be demonstrated in accordance with the Verification and Validation and Safety and Security Certification Program requirements identified in Chapter 7 of this SSMP.

Mitigation measures shall be applied in accordance with the *Prevention through Design* principle as detailed in Section 5.1. The *Prevention through Design* principle includes the following elements in order of precedence:

1. Avoidance
2. Elimination
3. Substitution
4. Engineering Controls
5. Warnings
6. Administrative Controls such as Operations and Maintenance Procedures
7. Personal Protective Equipment and Guards

Unacceptable risk will be reduced to an acceptable level before design acceptance. Undesirable risk must be reduced where reasonably practicable, and an Authority decision is required to accept the residual risk of the hazard or dispose of the system. The hazards will be reviewed by the SSPC, with recommendation made to the SSEC for decision. Acceptance of the level of risk or disposal of the system will be provided by the Authority through the SSEC. Tolerable risk can be tolerated and accepted with adequate controls, although risk-reducing mitigations must be applied where reasonably practicable. The iterative risk assessment process can be considered as completed when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered.

As a criterion, risks resulting from hazards may be classified as acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgment shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.

Individual hazards can be closed out by the application of one of the three principles, but it is likely that for most major projects a combination of the three principles will be used. Any risk assessment conducted under the CSM should always be proportionate to the extent of the risk being assessed. The CSM has been introduced to ensure that levels of safety are maintained or improved when and where necessary and reasonably practicable. Applying one or more of the three risk acceptance principles correctly for all identified hazards means that the risk has been reduced to an acceptable level. No further evidence is required to show that the residual risk is acceptable.

4.2.4.1 Application of Codes of Practice

The Authority shall analyze whether one or several hazards are appropriately covered by the application of relevant codes of practice.

The codes of practice shall satisfy at least the following requirements:

- Be widely acknowledged in the passenger rail industry. If this is not the case, the codes of practice will have to be justified and be acceptable to the Authority.
- Be relevant for the control of the considered hazards in the system under assessment.
- Be publicly available.

If one or more hazards are controlled by codes of practice fulfilling the requirements of points above, then the risks associated with these hazards shall be considered as acceptable. This means that these risks need not be analyzed further, however the use of the codes of practice shall be registered in the CEHL as safety requirements for the relevant hazards.

The PHA form developed during the hazard identification phase shall be completed with the term "acceptable" in the Resolution column. It will not be necessary to identify a final risk index.

Standards and rules that are widely accepted in the passenger rail sector include the following:

- Federal Railroad Administration regulations found in 49 CFR, Parts 200-299
- Federal Transit Administration regulations
- AREMA Standards for track
- California Public Utilities Commission General Orders
- TSIs or other mandatory European standards and norms
- Standards issued by the American National Standards Institute (ANSI)

This list is not exhaustive. It is also possible to use standards or codes of practice from other sectors (for example aviation, maritime, etc.) but these have to be justified and be acceptable to the ISA.

Deviations from codes of practice are possible where the Hazard Assessor can demonstrate that at least the same level of safety will be achieved. Mandatory standards such as FRA regulations often include a process for deviating from them. Most non-mandatory standards do not have a process for deviating from them. If one or more conditions of the code of practice are not fulfilled, the Hazard Assessor may have to conduct explicit risk estimation on those hazards where the code of practice is not relevant for the control of the hazards in the system under assessment. Alternatively, other codes of practice or reference systems could be used. Where an alternative approach is not fully compliant with a code of practice, the Hazard Assessor shall demonstrate that the alternative approach taken leads to at least the same level of safety.

If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional mitigation measures shall be identified applying one of the two other risk acceptance principles.

When all hazards are controlled by codes of practice, the hazard management process may be limited to the following:

- The hazard identification and classification in accordance with Section 4.2.3
- The registration of the use of the codes of practice in the CEHL
- The documentation of the hazard management process in accordance with Section 4.2.7

4.2.4.2 Use of a Reference System

The Authority, with the support of other involved actors, shall analyze whether one or more hazards are covered by a similar system that could be taken as a reference system. Reference systems can be used to derive the safety requirements for the new or changed system.

A reference system shall satisfy at least the following requirements:

- It has already been proven in-use to have an acceptable safety level and would still qualify for approval by the regulatory body having jurisdiction.
- It is accepted by the body having regulatory authority over its application to CHSTS (e.g., FRA, CPUC, Office of State Fire Marshal, etc.).
- It is used under similar functional, operational, and environmental conditions and has similar interfaces as the system under consideration for CHSTS.

For technical changes, it is unlikely that evidence of in-service history alone can prove that a high integrity system has an acceptable safety level, given the low failure rates required of such systems. Evidence that sufficient safety engineering principles have been applied in the development of the reference system will need to be confirmed for each application of it.

If a reference system fulfills the requirements listed above, then for the system under assessment the risks associated with the hazards covered by the reference system shall be considered as acceptable.

If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable.

If the same safety level as the reference system cannot be demonstrated, additional mitigation measures shall be identified for the deviations, applying one of the two other risk acceptance principles.

The safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system. These safety requirements shall be registered in the CEHL as safety requirements for the relevant hazards.

The PHA form developed during the hazard identification phase shall be completed with the term “acceptable” in the Resolution column. It will not be necessary to identify a final risk index.

When hazards are accepted by use of a reference system, the hazard management process may be limited to the following:

- The hazard identification and classification in accordance with section 4.2.3
- The registration of the use of the reference system in the CEHL
- The documentation of the hazard management process in accordance with Section 4.2.7

4.2.4.3 Explicit Risk Estimation

Explicit risk estimation is an assessment of the risks associated with hazard(s), where risk is defined as a combination of the likelihood (or frequency of occurrence) and the consequence (or severity) of a hazard. Explicit risk estimation can be used where:

- The Authority is unable to address the hazards identified in the hazard identification stage of the CSM via a code of practice or comparison with a reference system;
- Deviations are necessary from codes of practice or reference systems; or
- The Authority needs to analyze the hazards and evaluate design principles or safety measures.

The estimation can be qualitative, semi-quantitative, or quantitative. The choice will be determined by factors such as availability of, and confidence in, quantitative data; the depth of analyses should be proportionate to the potential risks. Any risk assessment should follow a systematic and structured process. Qualitative hazard assessment shall be performed by technical experts with sufficient experience and qualifications relevant to the hazard under consideration.

The acceptability of the estimated risks shall be evaluated using the risk acceptance criteria identified in Section 4.2.5. The acceptability of the risk may be evaluated either individually for each associated hazard or globally for the combination of all hazards considered in the explicit risk estimation.

If the estimated risk is not acceptable, additional mitigation measures shall be identified and implemented in order to reduce the residual risk to an acceptable level. The ALARP Principle (As Low as Reasonably Practicable) shall be applied to compare the cost and feasibility of applying additional mitigation measures against the benefit gained from reduced residual risk.

When hazards are accepted by use of explicit risk estimation, the hazard management process may be limited to the following:

- The hazard identification and classification in accordance with section 4.2.3
- Completion of the PHA process by registering the risk index in the Residual Risk Index (Projected) column of the PHA form
- The registration of the use of the explicit risk estimation and the mitigation measures in the CEHL; and
- The documentation of the hazard management process in accordance with Section 4.2.7.

When the risk associated with one or a combination of several hazards is considered as acceptable, the identified mitigation measures shall be registered in the CEHL.

Where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system, the following risk acceptance criterion shall apply for the design of the technical system:

- For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the failure rate of that system is less than or equal to 10^{-9} failures per operating hour.

The explicit risk estimation and evaluation shall satisfy at least the following requirements:

- The methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes).
- The results shall be sufficiently accurate to serve as robust decision support, i.e., minor changes in input assumptions or prerequisites shall not result in significantly different requirements.

4.2.5 Risk Estimation Process and Risk Acceptance Criteria

The risk assessment process for significant hazards is as follows:

1. Identify the hazardous event(s) that have the potential to cause injury or death to passengers, employees, or members of the public who are directly or indirectly exposed to the technical, operational, or organizational change being considered.
2. Identify the precursors (i.e., the component, sub-system or system failures, physical effects, human error failures or operational conditions) that can result in the occurrence of each hazardous event.
3. Identify the control measures that are in place to control or limit the occurrence of each precursor that cannot be eliminated.
4. Estimate the frequency at which each hazardous event can occur.
5. Estimate the consequences (most reasonable credible mishap) in terms of injuries and fatalities, environmental impact, monetary loss, or reputational damage that could occur for the different outcomes that may follow the occurrence of a hazardous event.
6. Estimate the overall risk associated with the hazardous event.

7. Identify additional mitigations or control measures that, if applied, would ensure that residual risk is reduced so far as is reasonably practicable.
8. Provide clear and comprehensive documentary evidence of the methodologies, assumptions, data, judgments, and interpretations used in the development of the risk assessment and the analysis of its results. Particularly where the assessment is quantitative and where different safety measures need to be assessed, the results may also need to be accompanied by sensitivity and uncertainty analysis.

The severity category and frequency of occurrence of the potential mishap(s) for each hazard across all system modes are estimated using the definitions in Table 4-1 and Table 4-2 respectively.

Table 4-1 Hazard Severity Categories

Hazard Category	Definition
1 Catastrophic	Could result in one or more of the following: • Multiple fatalities or equivalent fatalities • Irreversible significant environmental impact • Monetary loss equal to or exceeding $10M o Severe damage or total loss of rolling stock o Severe damage to infrastructure or other severe system loss causing all or a significant portion of the system to be unavailable for normal service for more than 72 hours • Reputational damage of national impact
2 Critical	Could result in one or more of the following: • A single fatality or multiple major injuries or occupational illnesses • Reversible significant environmental impact • Monetary loss equal to or exceeding $1M but less than $10M o Major but repairable damage to rolling stock o Major damage to infrastructure or other major system loss, repairable within 72 hours to allow normal service • Reputational damage of statewide impact
3 Marginal	Could result in one or more of the following: • A major injury or occupational illness, or multiple minor injuries • Reversible moderate environmental impact • Monetary loss equal to or exceeding $100K but less than $1M o Minor repairable damage to railcars o Minor damage to infrastructure or other minor system loss, repairable within 24 hours to allow normal service • Reputational damage of local area impact
4 Negligible	Could result in one or more of the following: • A minor injury or occupational illness • Minimal environmental impact • Monetary loss less than $100K o Minimal infrastructure damage or system loss affecting normal service for less than 12 hours • Reputational damage of limited or little impact

To determine the appropriate severity category as defined in Table 4-1 for a given hazard at a given point in time, identify the potential for death or injury, environmental impact, monetary loss, or reputational damage in a most reasonable credible mishap scenario. A given hazard may have the potential to affect one or all of these areas. An equivalent fatality may be expressed as 10 major injuries (those requiring hospitalization) or 100 minor injuries (those not requiring hospitalization).

Hazard frequency is defined as the likelihood that a specific hazard will occur during the planned life-cycle of the system element, subsystem, or component, recognizing that these life-cycles will vary depending upon the item under consideration. Hazard frequency can be described subjectively in potential occurrences per unit of time (Mean Time to Hazardous Event – MTTHE), events, population, items, or activity, and shall be ranked as shown in Table 4-2.

Table 4-2 Hazard Frequency Categories

Description	Level	Qualitative Definition	Qualitative Description for the System	Quantitative Context (Probability of Occurrence)
Frequent	A	Likely to occur frequently in an individual item or the System; may be continuously experienced in fleet/inventory.	MTTHE < 2 months	$p > 10^{-1}$
Probable	B	Likely to occur several times in the life of an individual item or the System; will occur frequently in fleet/inventory.	2 months < MTTHE < 1 year	$10^{-1} > p > 10^{-2}$
Occasional	C	Likely to occur sometime in the life of an individual item or the System; will occur several times in fleet/inventory.	1 year < MTTHE < 10 years	$10^{-2} > p > 10^{-3}$
Remote	D	Unlikely but possible to occur in the life of an individual item or the System; unlikely but can be expected to occur in fleet/inventory.	10 years < MTTHE < 100 years	$10^{-3} > p > 10^{-6}$
Highly Unlikely	E	So unlikely that it can be assumed occurrence may not be experienced in the life of an individual item or the System; unlikely but possible to occur in fleet/inventory.	MTTHE > 100 years	$10^{-6} > p$
Eliminated	F	Incapable of occurrence. This level is used when potential hazards are identified and later eliminated.	n/a	p = 0

Note - Frequency level F is used to document cases where the hazard is no longer present. No amount of doctrine, training, warning, caution, or Personal Protective Equipment (PPE) can move a mishap frequency to level F.

The frequency of the hazard can be determined qualitatively based on the relative frequency of expected occurrence, or quantitatively (using failure rates or accident/incident statistical data). Quantitative determination is generally preferable, but in the absence of applicable quantitative data the use of qualitative estimation is necessary and appropriate. Table 4-2 identifies both a qualitative definition and a qualitative description of the system using MTTHE, based upon a railway operation 20 hours per day, 7 days per week.

Hazard severity categories (1 through 4) and hazard frequency categories (A through E) are combined in the Risk Assessment Matrix (Table 4-3) to produce a risk index for each identified hazard. The Risk Acceptance Matrix (Table 4-4) identifies required actions to reduce risk based on the risk rating. The Authority will accept the residual risk through the Safety and Security Executive Committee process (where appropriate) through direct approval of individual risk acceptance decisions for hazard risks categorized as *Undesirable*. Hazard risks categorized as *Acceptable* do not require direct SSEC

approval, however review of the risk assessment process will fulfill the Authority's responsibility to accept the residual risk.

Table 4-3 Risk Assessment Matrix

Frequency \ Severity	1 Catastrophic	2 Critical	3 Marginal	4 Negligible
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Highly unlikely	1E	2E	3E	4E
(F) Eliminated				

Table 4-4 Risk Acceptance Matrix

Hazard Risk Index	Risk Rating	Action Required
1A, 1B, 1C, 2A, 2B, 3A	**Unacceptable**	Risk must be reduced and managed
1D, 2C, 2D, 3B, 4A	**Undesirable**	Risk is acceptable only where further risk reduction is impracticable. Authority decision at the SSEC level is required to accept residual risk.
1E, 2E, 3C, 3D, 4B	**Tolerable**	Apply mitigations where reasonably practicable. Risk can be tolerated and accepted with adequate controls. Authority review at the SSPC level is required to accept residual risk.
3E, 4C, 4D, 4E	**Acceptable**	No further risk reduction required
	Eliminated	None

4.2.6 As Low as Reasonably Practicable (ALARP Principle)

The ALARP Principle shall be applied where necessary to assess the cost/benefit of applying additional measures of mitigation in order to achieve residual risk that is as low as reasonably practicable. ALARP calculations can be qualitative, semi-quantitative, or quantitative depending on the level of risk and the amount of data available to the assessor. Qualitative analysis is entirely appropriate for assessment of risks that are found in standard industry practice or common experiences. Hazards deemed appropriate for more quantitative analysis will require development of more comprehensive analysis to provide the required level of data. Criteria for applying a detailed, quantitative cost/benefit analysis includes high risks that must be mitigated and accepted, highly-controversial risks, risks with a potentially high impact to the System or project under consideration.

The ALARP principle considers the fact that infinite time, effort and money could be spent on the attempt of reducing a risk to zero, but doing so is usually not practical. The principle is not simply a quantitative measure of benefit against detriment; it is more accurately a best common practice of judgment of the balance of risk and societal benefit. ALARP does not represent zero risk.

For a risk to be ALARP it must be possible to demonstrate that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained; that is the greater the risk, the more resources that should be spent in reducing it, and the greater the bias on the side of safety. The costs could marginally outweigh the benefits and yet the measure could still be reasonably practicable to introduce in order to reduce risk.

The disproportion factors (DF) in Table 4-5 shall be applied to the ALARP process according to the amount of risk. DFs that may be considered gross vary from upwards of 1 depending on a number of factors including the magnitude of the consequences and the frequency of realizing those consequences, i.e., the greater the risk, the greater the DF.

Table 4-5 Disproportion Factors for Risk

Risk Rating	DF
Unacceptable	10
Undesirable	8
Tolerable	5
Acceptable	1

When using a cost/benefit analysis, convert both the additional mitigation(s) and the risk (so far as it is being reduced) to a common set of units (dollars) for the purpose of making a comparison. A hazard is considered ALARP using a cost/benefit analysis when cost divided by the benefit is greater than the DF.

Other issues to consider when performing a cost/benefit analysis include the sensitivity of key inputs (frequency/severity of the hazardous event), animalization (average costs and average benefits), and discounting the value of future benefits.

4.2.7 Hazard Analysis Processes and Documentation, Verification and Validation

A variety of hazard analysis processes are available for proper risk estimation and mitigation development, based upon the characteristics of the system or subsystem under consideration. The types of analyses that may be required for the development of the CHSTS are described below.

- Preliminary Hazard Analysis (PHA) is typically the initial hazard analysis technique used during the system or subsystem design phase. PHA is used to identify safety critical areas within the system and roughly evaluate hazards. PHA establishes the basis for the safety criteria in design, equipment, and performance specifications.
- Site-Specific Hazard Analysis (SiSHA) is an expansion of the PHA, conducted as the general design criteria and system requirements are applied to specific system and subsystem elements. An

example would be a SiSHA for an elevated structure spanning the SR-99 highway in Fresno, applying the safety-critical criteria found in the Design Criteria to the specific characteristics and site conditions of this structure. SiSHA is generally performed during the Final Design, Construction, and Testing/Startup Phases. The primary output of the SiSHA is the identification and evaluation of hazards and mitigations that are specific to the system element under consideration.

- Failure Modes and Effects Analysis (FMEA) is an inductive analysis used to identify equipment failures. It evaluates a system or subsystem to identify possible failures of each individual component in the system. The results or effects of the subsystem and component failures are then classified according to severity.
- Fault Tree Analysis (FTAn) is representative of the deductive process. The purpose of the Fault Tree Analysis is to provide a concise and orderly description of the various combinations of possible occurrences within the system that can result in an undesired event. This is the most rigorous of the hazard identification processes and analyses and is typically performed for the most complex systems.
- Interface Hazard Analysis (IHA) is performed to identify design hazards in components and subsystems of a major system as they relate to other components or subsystems. IHA determines the functional relationships between the systems, subsystems, processes, components and equipment based solely on safety considerations and also identifies all elements in which a functional failure could result in a hazardous condition or accidental loss.
- Operating Hazard Analysis (OHA) is performed to determine all applicable operational safety requirements for personnel, procedures, and equipment throughout all phases of the system life cycle. Engineering data, procedures, and instructions developed from other safety analyses, the engineering design, and initial test programs are used to support this analysis.
- Software Hazard Analysis (SHA) will be used to evaluate software design, related software, and hardware documentation for safety-critical software-controlled functions. The analysis will review software and hardware failures that could cause the system to operate in a hazardous manner.
- Adjacent Railroad Hazard Risk Assessment Model (ARHRAM) will be used to assess the hazards associated with freight railroad right-of-ways directly adjacent to the CHSTS trackway. This is a semi-quantitative assessment process that relies on input from technical experts to assess site-specific characteristics of the adjacent railway.

The detailed process for completing each of these analysis types, including the appropriate forms, is identified in SSMP Appendix I. Appropriate support documentation used in the development of risk assessment will be identified or referenced in detail as part of each analysis process, including, but not limited to, the following:

- System description including modes of operation and tasks
- Schematics, drawing, block diagrams, lists of assemblies, parts and components addressed within each subsystem and system
- Documented reliability and safety data including failure rate data obtained from service use in identical or manifestly similar equipment in similar environment
- Documented reliability and safety data obtained from formal test results, conducted in similar applications
- Documented reliability and safety data obtained from formal analyses, conducted for equipment in similar applications
- Hazard management requires monitoring and documentation throughout the project life cycle. Verification and validation activities shall fulfill the requirements of the Safety and Security Certification Program, as described in Section 7 of this SSMP.

4.3 Security Risk Assessment Process

Planning in advance of day-to-day passenger rail crimes, terrorist acts, or other security incidents is essential to providing CHST passengers and employees with a safe and secure environment. A breach in security may result in serious injuries or death, destruction of property and facilities, and/or the inability to continue CHSTS operations to the region.

Adopting a methodology that involves periodic assessment is consistent with the requirement of the system security lifecycle and ISO 31000 Risk Management standard.

In order to ensure that the Authority has considered security risks, such as crime or acts of terrorism, it is crucial to apply a methodological approach and process to security risk management. The risk assessment process that will be used (and as illustrated in Figure 4-2) includes the following:

- Identify the key assets
- Identify the threats
- Identify the vulnerabilities
- Identify the likelihood
- Identify the consequence/impact
- Assign the initial risk index as the basis for future risk decision criteria
- Identify potential mitigation measures/countermeasures
- Determine residual risk after implementation of countermeasures

Figure 4-2 Security Risk Assessment Process

To evaluate the susceptibility to potential threats and to design corrective actions that can reduce or mitigate the risk of serious consequences from a security incident, a Threat and Vulnerability Assessment (TVA) will be initiated during the preliminary phases of the CHSTS. The assessment will be reviewed and updated at each subsequent phase.

The TVA process will identify the likelihood of specific threats that may endanger railroad assets (people, property, and information); the potential vulnerabilities associated with the design of the CHSTS; and mitigation efforts that can be designed into the CHSTS to reduce the risk and to minimize the consequences of identified potential criminal and terrorism activities. It will also identify future security training needs of transit personnel and the necessity for security procedures. The Security Risk Assessment will be protected under Sensitive Security Information (SSI) and shared *only* with those persons with a need to know.

4.3.1 Assets

4.3.1.1 Identification

Assets are defined as people and property. System assets include the following:

- People – passengers, employees, visitors, contractors, vendors, surrounding communities, and others who come into contact with the transit system
- Property – fixed infrastructure, rolling stock, software
- Information – plans, procedures, network information, passwords and access codes

Assets associated with the CHSTS will be identified during the TVA process and included as a listing in the Threat and Vulnerability Assessment Report.

4.3.1.2 Criticality Determination

Assets will be prioritized in terms of criticality. Most weight will be given to those assets that present the greatest threat to life safety or service disruption. In making this determination, consideration will be given to the following:

- Impact on CHSTS passengers, employees, and first responders
- Impact on CHSTS operations
- Economic value of the asset, including current and replacement value
- Intrinsic value of the asset to a potential adversary
- Asset location relative to other critical assets

4.3.2 Identification of Threats

Threats are defined as deliberate actions intended to cause injury or death to people or damage or loss of critical assets. The threats (or attack types) to the CHSTS will generally be the same as those faced by other public transportation networks. Threat is the combination of both intent and capability of a threat actor or threat source to realize a threat or attack against an asset. It is possible to separately analyze the intent and the capability but this type of analysis requires specific information and intelligence about specific threat actors.

As part of the security risk management system it is important to understand target attractiveness. Target attractiveness varies depending upon threat actor motivations and goals, but in general the following criteria are useful in determining the potential for target selection:

- Potential for public impact, damaging the society and ecosystem as a whole
- Lack of target protection and does the target follow predictable patterns
- Potential for mass casualties
- Potential for global significance or visibility to either the threat actor or the target
- Target permanently or frequently available
- Potential for major political or economic impact
- Potential for economic gain
- Ease of accessibility
- Perceived “iconic” status

Determination of security threat is always evolving and requires analysis to be based on the past performance of threat actors, both successful and attempted. Historical data (from reliable open source information) of manifested threat events across national and international transit systems provides accurate data to enable security threats to the CHSTS assets and systems to be established.

A series of tables illustrate examples of threat categories (Table 4-6), crime categories (Table 4-7), and threat types (Table 4-8).

Table 4-6 Threat Category Examples

Threat Category	Sources
Criminal	Petty crime Organized crime Current/former staff
Terrorism	Domestic extremist groups Transnational extremist groups Single-issue groups
Hostile State	Military State-sponsored hostile actors

Table 4-7 General Crime Categories and Examples

Threat Category	Crime Types within Category
Crimes against Persons	Assault, homicide, robbery, theft
Crimes against Property	Arson, cargo theft, vandalism, burglary
Other Crimes committed on Transit Property	Organized crime presence – infiltrating rail system, using rail system to move contraband, drugs, prostitution, fare evasion, trespass

Table 4-8 Threat or Attack Types Examples

Threat Type	Types within Category
Explosives	Military explosive, improvised explosive device (IED), vehicle-borne improvised explosive device (VBIED), personnel-borne improvised explosive device (PBIED)
Chemical	Toxic industrial chemicals, and poisons
Arson	Incendiary Devices
Small Arms Attack	Use of standard firearms and other weapons
Standoff Attack	Weapons with high-energy explosives that are designed to hit and penetrate heavily protected objects from a distance.
Cyber Attack	Viruses, Worms and Trojan Horses
Hoax Call or Device	Intentional false alarm or threat

As stated previously, threat is based upon the combination of intent and capability. Table 4-9 provides the threat rating matrix and Table 4-10 provides the threat ratings and their descriptions.

Table 4-9 Threat Rating Matrix (Intent x Capability)

INTENT	CAPABILITY				
	Similar exploit has been used	Operational capability confirmed by credible evidence	Some evidence that operational capability exists; not confirmed	No evidence of operational capability but feasibility confirmed	No evidence and even feasibility unconfirmed
Tactic has been used in the past and a similar attack may be planned	**Very High**	**Very High**	**High**	**Medium**	**Low**
Tactic has been used before and it is credible that it is being considered for further use	**Very High**	**High**	**High**	**Medium**	**Low**
Tactic has not been used before but is under consideration	**High**	**High**	**Medium**	**Medium**	**Low**
Tactic has not been used before but it may be under consideration	**Medium**	**Medium**	**Medium**	**Low**	**Very Low**
Tactic has not been used before and is not known to be under consideration	**Low**	**Low**	**Low**	**Very Low**	**Very Low**

Table 4-10 Threat Rating and Definitions

Threat Rating	Threat Rating Definition
VERY HIGH	Significant and proven threat present based upon demonstrated intent and demonstrated capability
HIGH	Threat present based upon stated/demonstrated intent with demonstrated capability.
MEDIUM	Medium level threat exists based upon either strong intent or some degree of stated/demonstrated capability.
LOW	General threat exists and should be monitored – no proven intent or demonstrated capability
VERY LOW	General threat may exist with intent and capability feasibility unconfirmed

For purposes of the CHST System, threat of terrorist activity will be based on information provided by DHS/TSA and other credible sources. For other threats, including crime and quality of life incidental threats, the Security Risk Assessment will review crime data provided by law enforcement in the adjacent areas, and open source data of criminal threats for other rail systems.

4.3.3 Scenario Analysis

Scenarios are the outcome of pairing specific assets with specific threats. An explosive device at a rail station provides a scenario that can be evaluated to identify the vulnerabilities that may make the rail station, an identified asset, susceptible to an attack. Scenario development also identifies impacts of

threats on critical assets and promotes mitigation strategies and capability needs. The scenarios are intended to represent credible, real-world events and, as such, will be derived primarily from other operating systems' experiences, FTA and TSA resource documents, and local crime report information.

4.3.4 Identification of Vulnerabilities

Vulnerability is defined as any weakness, flaw or condition that allows and/or can be exploited, for the successful realization of a potential threat against the CHSTS. In general, vulnerability conditions allow access to an asset in order to be attacked. As the threat environment is ever changing, vulnerabilities to different threats and attack methods may also change, which requires updated review of the threats, vulnerabilities and the consequences. However, by addressing known vulnerabilities and therefore limiting the associated consequences of a potential threat, the likelihood of having to make significant changes is reduced for future updates.

Vulnerability conditions can be classified into two different types, physical, and procedural. A physical vulnerability condition is an actual physical deficiency, flaw, or absence of physical measures designed to deter, detect, delay, and/or respond against a breach or unauthorized access to an asset. A procedural vulnerability condition relates to the existence, implementation, legality, and oversight of policies and procedures, which are designed to deter, detect, delay, or respond against a breach or unauthorized access to an asset.

Successful execution of an attack type is dependent upon the presence of either a physical vulnerability, or a procedural vulnerability, or both. By identifying the physical and procedural conditions that contribute to a certain threat type and attack method, it is possible to start developing general mitigation strategies to address the vulnerability and therefore reduce the likelihood and/or consequences of a successful attack.

In a new project, the assumption is that the system is completely without mitigations measures, but takes into account typical operating features and assets. Any countermeasures that might impact a perceived vulnerability will be recommended for implementation into the design and construction. Assessments performed on existing systems look for the weaknesses in an existing design or system.

Table 4-11 details the vulnerability levels used as part of the vulnerability determination.

Table 4-11 Vulnerability Levels and Description

Vulnerability Level	Assessment Criteria
Very High	• Non-existent advanced physical and procedural mitigation measures • Inadequate existing mitigation measures; and will likely fail to deter, detect, delay, or respond to a security risk • No security awareness culture present • No business or operations contingencies to manage security events and recover. Severe disruptions are likely
High	• Some physical and procedural mitigation measures, but ineffective at deterring, detecting, delaying, or responding to advanced security risks • More than 50% of existing mitigation measures are likely to fail to deter, detect, delay, or respond to a basic security risk • No security exercises performed or planned • Few contingencies/plans are in place for business and operations recovery. Significant disruptions likely
Moderate	• 50% of advanced physical and procedural mitigation measures are effective with remaining measures likely to fail to deter, detect, delay, or respond to a security risk • Existing mitigation measures are capable of deterring, detecting, delaying, and responding to basic security risks • Exercise program exists and exercises are performed for select areas • Basic security awareness culture • Contingencies/plans are in place across most but not all key areas of business and operations, but require improvement. Some disruptions are likely
Low	• 50% - 80% of advanced physical and procedural mitigation measures are effective but some improvements are required • Existing mitigation measures are capable of deterring, detecting, delaying, and responding to basic security risks • Procedures and evidence (records) of audit and review of existing security measures • Exercise program exists and exercises are performed for select areas • Cultivation of security awareness culture is a primary objective of management • Business and operations contingencies plans are in place for all key areas to manage security events and recover
Very Low	• 80% or higher effectiveness of advanced physical and procedural mitigation measures to deter, detect, delay, and respond to security risks and are sustainable • Procedures and evidence (records) of audit and review of existing controls • Exercise program exists and exercises are performed for select areas • Security awareness culture is integrated into all business activities • Comprehensive contingency plans in place across entire business and operations to manage most identified disruptions

4.3.5 Determining Likelihood

Likelihood is the combination of threat and vulnerability. Table 4-12 describes the combination of the threat and vulnerability to create the likelihood rating and index.

Table 4-12 Likelihood Determination Matrix (Threat x Vulnerability)

Threat	Vulnerability				
	Very High	High	Moderate	Low	Very Low
Very High	Almost Certain	Almost Certain	Highly Likely	Likely	Likely
High	Almost Certain	Highly Likely	Highly Likely	Likely	Possible
Medium	Highly Likely	Likely	Likely	Possible	Possible
Low	Likely	Likely	Possible	Possible	Remote
Very Low	Possible	Possible	Possible	Remote	Remote

The likelihood is based upon the definitions in Table 4-13.

Table 4-13 Likelihood Rating and Definitions

Likelihood Rating	Likelihood
	Characteristics
Almost Certain A	Vulnerability exists and threat is proven and demonstrated. Threat realization can be expected to occur during the system's operational phases
Highly Likely B	Vulnerability exists and threat is proven although may not be demonstrated. Threat realization may be expected during system's operational phases
Likely C	Some vulnerability exists and threat has some resource, experience, and skill, though may not be demonstrated. Threat realization may occur during the system's operational phases
Possible D	Limited vulnerability exists and threat may be under resourced and may lack experience and skill, should not occur during the system's operational phases
Remote E	Limited vulnerability exists or threat has not been proven or demonstrated, not expected during the system's operational phases

4.3.6 Determining the Consequence

Consequence is the assessed impact and severity of a successful threat against an asset, the system, or network. Consequence is measured by the level of impact on primary areas of people, equipment or service and finances. Reputational impacts can also be assessed. Examples of consequences include injuries to the public or to CHSTS personnel, loss of equipment causing financial losses, and disruption to CHSTS operations. Reputational damage occurs when the system is considered unsafe or dangerous, impacting ridership, and funding. Severity categories are defined to provide a qualitative measure of the result of a security breach and are summarized in Table 4-14.

Table 4-14 Consequence Ratings and Assessment Criteria

Severity Rating	CHARACTERISTICS			
	People	Equipment or Services	Financial	Reputational
Catastrophic 1	Several deaths and/or numerous severe injuries	Total loss of equipment or system interruption requiring months to repair	Estimated loss in excess of $5 million	Ongoing international, national media coverage, severe reputational damage, government intervention, Weeks - Months
Critical 2	Low number of deaths (less than 3) and/or severe injuries	Significant loss of equipment or system interruption, requiring weeks to repair	Estimated loss from the incident expected to range from $500,000 to $5 million	Prolonged national and local media, serious reputational damage, sustained government involvement, Days-Weeks
Moderate 3	Possible severe injury or several minor injuries	Loss of equipment or system interruption, requiring seven or less days to repair	Estimated loss from the incident expected to range from $50,000 to $499,999	Adverse national and local media coverage, reputational damage, government involvement
Minor 4	Possible minor injuries or illness	Minor loss of equipment, no system interruption, less than 24 hours to repair	Estimated loss from the incident expected to be minor, $1000 to $49,999	Local media coverage and some reputational damage
Negligible 5	No injuries or illness	Minor damage to equipment, no system interruption, no immediate repair necessary	Estimated loss less than $1000	No adverse media coverage or reputational damage

4.3.7 Security Risk Criticality Matrix

The consequence, or severity, of a threat and the likelihood of occurrence will be combined into a risk level criticality matrix. The consequences will be assessed both in terms of severity of impact and probability of occurrence for a given threat. The criticality matrix organizes the resulting consequences into categories of high, serious, and low. The matrix will help to prioritize risk to focus available resources on the most serious threats requiring resolution while effectively managing the available resources. The Security Criticality Matrix is shown in Table 4-15.

Table 4-15 Security Risk Criticality Matrix (Likelihood X Consequence)

Consequence Severity	Likelihood				
	Almost Certain A	Highly Likely B	Likely C	Possible D	Remote E
Catastrophic – 1	Very High 1A	Very High 1B	High 1C	High 1D	Moderate 1E
Critical – 2	Very High 2A	High 2B	High 2C	Moderate 2D	Moderate 2E
Moderate – 3	High 3A	High 3B	Moderate 3C	Moderate 3D	Low 3E
Minor – 4	Moderate 4A	Moderate 4B	Moderate 4C	Low 4D	Very Low 4E
Negligible – 5	Low 5A	Low 5B	Low 5C	Very Low 5D	Very Low 5E

Source: Adapted from FTA's Public Transportation System Security and Emergency Preparedness Planning Guide

Once the risk rating is determined for each security risk to each identified asset, then the risk index at Table 4-16 can be used to determine and prioritize the resources and financial justification for risk treatment.

Table 4-16 Security Risk Index

Risk index	Risk Rating	Action Required
1A, 1B, 2A	VERY HIGH	Risk must be immediately mitigated and constantly monitored
1C, 1D, 2B, 2C, 3A, 3B	HIGH	Risk must be treated and monitored, Authority decision at the SSEC level is required to accept risk.
1E, 2D, 2E, 3C, 3D, 4A, 4B, 4C	MODERATE	Risk should be managed and reduction strategies implemented. Authority decision at the SSPC level is required
3E, 4D, 5A, 5B, 5C	LOW	Risk may be accepted after a risk review by the SSPC
4E, 5D, 5E	VERY LOW	Risk would normally not be treated

Source: Adapted from FTA's Public Transportation System Security and Emergency Preparedness Planning Guide

4.3.8 Countermeasure Development

After determination of the risk, countermeasures or corrective actions are developed that can mitigate or eliminate the risk. Effective countermeasures can either be design or procedural or a combination. Examples of design or engineered countermeasures include the following:

- Installing physical barriers designed to reduce the asset's vulnerability to unauthorized access, explosive, or other incendiary attacks
- Installing integrated intrusion detection and alarm systems throughout key facilities
- Installing chemical, biological, radiological and/or nuclear detection devices at facility and station locations

Procedural or Administrative countermeasures include the following:

- Increasing the frequency of security patrols at key asset locations
- Increasing security-related training to improve the abilities of employees to identify suspicious packages or activities
- Conducting emergency exercises and drills involving security-related scenarios
- Developing working groups and information exchange committees with local law enforcement and emergency response agencies.

During the development of countermeasures, consideration will be given not only to the initial costs of procurement and implementation, but also to the associated maintenance costs and expected level of effectiveness at eliminating or controlling the threat and/or vulnerability. Cases where conditions may be exacerbated, such as special events, will be taken into account. During these conditions, ridership is likely to be greater than normal and may impact the effectiveness of the countermeasure.

4.3.9 Residual Risk

Residual risk refers to the risk remaining after application of the countermeasures. If the residual risk has not been reduced to an acceptable level, additional countermeasures or mitigation strategies must be considered.

4.3.10 Reporting

The assessment details are captured in worksheets or tables which define the major elements of specific scenarios. An example of a TVA worksheet is depicted in Figure 4-3.

Figure 4-3 Security Risk Worksheet Example

Rail Critical Assets															
ID NO.	Asset	Threat Type/ Event	Threat Rating	Vulnerability Condition		Vulnerab. Rating	Likelihood Index (Threat/ Vulnerability)	Potential Effect	Conseq. Index	Int. Risk Rating (Likelihood/ Conseq)	Potential Mitigation Measures	Res. Risk Rating	Verification & Validation		
				Procedural	Physical								Resp Party	Ref/ Status	Accept of Resolution
RV1	Rail Vehicle	VBIED Collides with a rail vehicle	Low	Absence of suspicious activity reporting and communication procedures	Lack of hostile vehicle mitigation (HVM) to prevent vehicles forcing entry through control points (Loading areas)	High	C Likely	Economic disruption to system and adjacent facilities	1 Catastrophic	1C HIGH	Training of uniform security force/police on threat environment and transportation security	1E MOD			
				Insufficient or absence of public area inspection	Lack of vehicle bollards and standoff at loading areas			Damage to equipment and facilities			Implementation of suspicious activity reporting and communication procedures				
				Lack of or insufficient training of uniform security force/police on threat environment and transportation security	Lack of access controls			Death and/or Injury			Random and continuous inspection and patrol of facility, personnel, and equipment by uniform security				
				Absence of ongoing liaison and exchange of security information with external security authorities				Operational disruption			Maintenance of ongoing liaison and exchange of security information with external security authorities				
								Reputational damage (external stakeholders)			Hostile vehicle mitigation (HVM) at vehicle access points (Loading areas) to prevent vehicles forcing entry; bollards and standoff at the Loading areas.				
								Reputational damage (internal stakeholders)			Right of Way access controls				

4.4 Verification and Validation Documentation

Each identified safety hazard and security risk will be managed to resolution through the Verification and Validation (V&V) methodology and documented in the Requirements Management Tool database system adopted by the CHSTS. The V&V methodology and documentation requirements are described in the CHSTS Verification and Validation Management Plan.

5.0 DEVELOPMENT OF SAFETY AND SECURITY DESIGN CRITERIA

5.1 Prevention through Design

Hazards can be resolved by deciding to either assume the risk associated with the hazard or to eliminate or control the hazard. The Prevention through Design principle, as identified in ANZI Z590.3-2011 *Prevention through Design*, incorporates safety and security considerations into the early design of a system element so as to avoid, eliminate, or mitigate hazard risk to a level as low as reasonably practicable. The following order of precedence shall be applied when incorporating safety considerations into design:

1. Avoidance. Develop concepts of operations, basis of design, or general system requirements to avoid the introduction of hazards to the system.
2. Elimination. Design, redesign or retrofit to eliminate (i.e., design out) the hazards through design selection. This strategy generally applies to acquisition of new equipment or expansion of existing systems; however, it can also be applied to any change in equipment or individual subsystems.
3. Substitution for Minimum Risk. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level. This may be accomplished, for example, through the use of fail-safe devices and principles in design, the incorporation of high-reliability systems and components and use of redundancy in hardware and software design.
4. Engineering Controls. Hazards that cannot be eliminated or controlled through design selection will be controlled to an acceptable level through the use of fixed, automatic or other protective safety design features or devices. This could result in the hazards being reduced to an acceptable risk level. Safety devices may be part of the system, subsystem or equipment. Examples of safety devices include interlock switches, protective enclosures and safety pins. Care must be taken to ascertain that the operation of the safety device reduces the loss or risk and does not introduce an additional hazard. Safety devices will also permit the system to continue to operate in a limited manner. Provisions will be made for periodic functional checks of safety devices.
5. Provide Warning Devices. When neither design nor safety devices can effectively eliminate nor will control an identified hazard, devices shall be used to detect the hazardous condition and generate an adequate warning signal to provide for personnel remedial action. Warning signals and their application will be designed to minimize the probability of incorrect personnel reaction to the signals and will be standardized within like types of systems. Warning signals and their application should also be designed to minimize the likelihood of false alarms that could lead to creation of secondary hazardous conditions.
6. Administrative Controls. Where it is not possible to eliminate or adequately control a hazard through design selection or use of safety and warning devices, procedures and training will be used to control the hazard. Special equipment operating procedures can be implemented to reduce the probability of a hazardous event and a training program can be conducted. The level of training required will be based on the complexity of the task and minimum trainee qualifications contained in training requirements specified for the subject system element and subsystem. Precautionary notations in manuals will be standardized. Safety critical tasks, duties and activities related to the system element and subsystem will require certification of personnel proficiency. However, without specific written approval, no warning, caution or other form of written advisory will be used as the only risk reduction method for unacceptable and undesirable hazards.
7. Personal Protective Equipment and Guards: Where no other higher-level alternative mitigations are possible, the use of personal protective equipment or the installation of guards will be used to mitigate the hazard. Personal protective equipment and guards may be used to supplement other higher-level mitigations, but when they are the only mitigation applied they are to be used only when no other alternatives exist.

5.2 Design Criteria

Design criteria are developed from the engineering experience of the design team obtained from numerous other rail projects, as well as the following sources:

- Formal hazard analyses, including Preliminary Hazard Analysis
- Threat and Vulnerability Assessments
- Federal Railroad Administration regulations found in Code of Federal Regulations Title 49, Parts 200-299
- California Public Utilities Commission (CPUC) General Orders
- California Building Code
- California State Fire Marshal's Office direction and recommendations
- Local building codes and Fire Marshal recommendations
- National Fire Protection Association (NFPA)
- American Public Transportation Association (APTA)
- American Railway Engineering and Maintenance-of-Way Association (AREMA)
- Underwriters Laboratories (UL)
- Safety and security recommendations of the Department of Homeland Security (DHS), Transportation Security Administration (TSA), and the Federal Transit Administration (FTA)
- Other industry or technical standards

CHSTS will conduct Preliminary Hazard Analysis and Threat and Vulnerability Assessment during the Preliminary Engineering phase to aid in defining safety and security design criteria.

Design criteria are developed to address system safety and security requirements applicable to the entire system. System safety and security requirements for each specific design element will be incorporated into a Design Manual chapter entitled *CHSTS Design Criteria* with reference to corresponding design criteria for specific engineering elements (e.g., clearances, structures, seismic criteria, etc.).

The processes described in the *CHSTS Verification and Validation Management Plan* (VVMP) will ensure that the design criteria and the basis of design report will incorporate safety and security requirements into the system design.

The following documents have been prepared by the PMT in order to achieve the system's design criteria's objectives:

- Basis of Design Report
- Risk Management Plan and Hazard Log
- System Requirements
- Infrastructure Maintenance Plan
- Technical Memoranda
- Design Criteria
- Standard Drawings
- Standard Specifications

A consistent approach will be utilized within all the engineering efforts and will assist the CHSTS Regional Consultant teams in preparation of their designs.

The *Basis of Design Report* defines the key CHSTS performance requirements. This document serves as the guiding force in establishing the design criteria and development of design standards. The key

audience for the Basis of Design Report is the Authority, the Program Manager, the Regional Project Managers, and the Section Designers. The purpose of the report is to guide the Engineering Management Team during the development of engineering criteria and provide the required performance levels for the CHSTS.

A *Risk Management Plan and Hazard Log* will be developed outlining methodologies to ensure that a consistent approach to risk assessment and cost are applied throughout the CHSTS. The plan will address both system safety risk and project delivery risk, and include a Program level risk register that will be regularly updated and maintained.

The *CHSTS System Requirements* provides a common platform for which similar Code of Federal Regulations, CPUC General Orders, and European Union Technical Specifications for Interoperability, as well as other industry best practice and standards, can be collectively presented and assessed at a detailed technical level. In addition to guiding and supporting specific technical guidance at the subsystem level, the CHSTS System Requirements structure is used to demonstrate how the performance objectives of the CHSTS are to be achieved.

Technical Memoranda have been prepared to describe detailed analysis of specific technical topics, and to provide guidance to the Regional Consultants in the development of Preliminary Engineering to support feasibility, environmental, and procurement efforts. Technical Memoranda are provided as information to Final Design teams, but are not considered mandatory requirements.

The *Infrastructure Maintenance Plan* is a base document outlining how the CHSTS will be maintained. This document sets forth the requirements for maintenance facilities for rolling stock and the railway infrastructure, as well as the approximate location and size of supporting facilities.

Design Criteria have been prepared that is intended to serve as the design requirements for a possible Design/Build consortium. The Design Criteria identifies and specifies required elements and considerations to ensure a safe and reliable operating railway for the CHSTS. The Design Criteria will be supported by *Standard Drawings* and *Standard Specifications* as required.

5.3 Design Reviews

CHSTS drawings and specifications will be reviewed informally during development and formally during preliminary and final design. The purpose of these reviews will be to verify conformance with all of the projects design criteria. These reviews are performed by the corresponding PMT discipline design personnel, their design supervisors, applicable oversight agencies, representatives from the Regional Consultants, and the PMT System Safety and Security staff.

Design reviews will be scheduled and coordinated so as to permit ample opportunity for comments and approvals. After satisfactory resolution of comments, the specifications are “sealed” by professional engineers from the Regional Consultants design group and issued for use.

5.4 Deviations and Changes

For any instances that arise requiring a possible deviation from the safety-critical or security critical design criteria (i.e., physical constraints identified within the system’s corridor conflicting with baseline requirements), the PMT and the associated segment Regional Consultant during Preliminary Engineering (and PMT and Design/Build Contractor during Final Design) will be required to explore all reasonable alternatives to provide a design that conforms to the requirements of the existing criteria. If a reasonable alternative cannot be developed, the requesting party will submit a Design Variance Request (DVR) to the PMT, whose members include safety and security personnel and representatives of the required engineering disciplines. The requesting party will be responsible for identifying and resolving any hazards or vulnerabilities related to any deviations.

Any deviations to the Design Criteria developed by the PMT or design/build contractors will require a safety and security assessment for each deviation to ensure that the same level of safety and security is achieved as would have occurred had the Design Criteria been followed. A formal hazard analysis and/or TVA may be required to support the safety and security assessment of Design Criteria deviations. If the

change request is approved, the findings and recommendations will be incorporated into the Final Design engineering and construction plans and the Final Design Verification Checklist(s) will be updated to reflect the change.

During the life cycle of the project, the SSPC may also confront design issues that require additional hazard analysis or vulnerabilities assessment, the outcome of which may result in requests for design changes. Such requests will be processed through the Design Variance Request process.

The PMT is responsible for monitoring all design requests/changes for compliance with the Design Criteria or Design Standards documents, including statutory and regulatory requirements and requirements specified in any contract. The Design Variance Process is described in Technical Memorandum 1.1.18 Design Variance Guidelines.

6.0 QUALIFIED OPERATIONS AND MAINTENANCE PERSONNEL

6.1 Operations and Maintenance Requirements

The Authority's Operations and Maintenance Team (OMT) will be responsible for developing system operations and maintenance requirements that support the safe and efficient operation of the California High-Speed Train system. Principal activities of the OMT include the following:

- Provide ongoing operations input to the Engineering Management Team and Regional Engineering teams in the development of system design elements
- Review and comment on engineering design elements to ensure responsiveness to operations' functional requirements
- Coordinate with FRA on development of CHSTS rules and procedures and their relationship to current regulations and new regulations that will emerge from the CHSTS. Key categories include:
  - Code of Federal Regulations (CFR) regulatory issues
  - Rail System Operating Rules
  - System Safety Rules and Procedures
  - Standard Operating Procedures
  - Emergency Action Plans and Procedures
  - Infrastructure /Systems maintenance and inspection procedures
  - Rolling Stock maintenance and inspection procedures
- Coordinate with railroads, operating agencies/rail service providers and stakeholders as required

Personnel staffing requirements for the operation and maintenance of the in-service CHSTS will be established and described in the *CHSTS Training and Personnel Qualification Plan*, to be developed prior to the startup of revenue operations.

Development of the *CHSTS Operations and Maintenance Plan* for any system or subsystem component will begin during Construction Phase. Position titles, responsibilities, qualifications, and training requirements will be identified consistent with other high-speed rail operating systems using similar technologies and operating characteristics. The magnitude of the in-service CHSTS (trains operated, vehicles in service, track and OCS systems to maintain) will determine staffing levels for operators, maintainers, and supervisors.

Additionally, the *CHSTS Infrastructure Maintenance Requirements Plan* (IMRP) establishes and describes how infrastructure maintenance will be planned and implemented including methods utilized and resources required. The IMRP specifies the CHSTS requirements necessary to meet passenger and public safety levels that meet or exceed FRA Class 6 Regulatory Safety Standards, consistent with FRA's High-Speed Passenger Rail Safety Strategy. IMRP requirements will be incorporated into the system Design Criteria during the Preliminary Engineering phase of the CHSTS.

6.2 Operations and Maintenance Plans, Rules and Procedures

The following documents will be revised for the CHSTS during the Project Construction Phase, in preparation for Testing and Startup:

- Concept of Operations
- Code of Operating Rules
- Rolling Stock Maintenance Plan
- Infrastructure Maintenance Requirements Plan
- Training and Personnel Qualification Plan
- Service/Operating Plan
- Command and Control Facilities Plan
- On-Board Operating Plan
- Passenger Station Operating Plan
- Passenger Train Emergency Preparedness Plan
- Air Brake Operating Instructions
- Electrical Operating Instructions
- Emergency Operating Procedures
- Timetable Special Instructions
- On-Track Safety Rules
- System Safety Program Plan
- System Security Program Plan
- Emergency Preparedness Plan

6.3 Training Program

The Authority intends to hire one or more concessionaires to provide rail operations and maintenance services. The Authority will be responsible for ensuring that the concessionaire(s) assign qualified O&M personnel to the CHSTS who are trained to perform pre-revenue and revenue operations. Instruction in safe methods of operation, safety requirements, security awareness and emergency response procedures will be included in manuals, handbooks, and other documentation developed for the training and certification of operations and maintenance personnel. Training plans, which include in-house classroom training and on-the-job training and testing, will be developed based on the individual characteristics of the equipment or CHSTS locations.

The future CHSTS Operators, Instructors and Field Supervisors will undergo familiarization training on all operational equipment, rules, plans and procedures. The future Central Control Operations Staff (including Superintendents, Supervisors, and Train Dispatchers) will require extensive training and qualification on the train control system, in addition to operating rules and procedures, and safety and security procedures.

Positions which will require detailed job descriptions and training programs prior to entering the Testing Phase of the CHSTS include, but are not limited to the following:

- Superintendents
- Operations Supervisors
- Train and Engine Service Employees
- Control Center Supervisors
- Control Center Train Dispatchers
- Equipment Maintenance Employees
- Signal and Communications Employees
- Maintenance of Way Employees
- Power and OCS Employees

Contractors and suppliers providing equipment and facilities for the CHSTS will be responsible for developing training plans, training manuals, and conducting training courses for applicable CHSTS Operations and Maintenance staff. Contractors will be required to develop and implement programs to train appropriate CHSTS personnel in the operation and maintenance of each piece of equipment or systems provided in conformance with the *CHSTS Training and Personnel Qualification Plan*.

6.4 Emergency Preparedness

A *Passenger Train Emergency Preparedness Plan* (PTEPP) will be developed prior to the start of the Testing Phase of the CHSTS to prepare for emergency incidents that may occur during testing. The PTEPP will be further developed and carried over into the start of revenue service. The PTEPP will contain emergency preparedness requirements and procedures for the Operations and Equipment Maintenance disciplines, in compliance with 49 CFR, Part 239. The PTEPP will identify requirements for a program of training (including instructional programs, emergency preparedness drills and tabletop exercises) of railroad operating and maintenance personnel and emergency responders. The goal of the PTEPP is to verify and validate the following:

- Adequacy of emergency plans and procedures
- Readiness of railroad operating and maintenance personnel to perform under emergency conditions
- Effective coordination between railroad operations and emergency response agencies: police, fire, and emergency medical services
- Familiarization of fire, police, and emergency medical services personnel with the physical and operating characteristics of CHSTS operations and inherent hazards

After-action reviews will be conducted following any major emergency response event or exercise prior to the start of revenue operations. A report of the findings will be provided to the SSPC. Action items will be tracked by the SSPC to completion through the V&V process. Outcomes may include recommendations for revisions to the PTEPP, operating rules or procedures, equipment or infrastructure changes, or emergency responder procedures, and changes to training plans and training programs pertaining to emergency response and personnel.

Fire/Life Safety and Security Committees will be established at both a regional and State level as described in Section 3.4.3 of this SSMP to provide a vehicle for clear, consistent communication with emergency responders.

7.0 SAFETY AND SECURITY CERTIFICATION PROGRAM

7.1 Overview

The California High-Speed Rail Authority is ultimately responsible for ensuring that all safety-critical and security-critical elements of the CHSTS are designed, constructed, tested, and made operationally ready in a safe and secure manner prior to the start of revenue service. The Safety and Security Certification Program describes the responsibilities and processes required to demonstrate that the CHSTS is safe and secure, in conformance to the FTA *Handbook for Transit Safety and Security Certification* and Federal Railroad Administration (FRA) Regulations 49 CFR 236, Sub-parts H and I for Positive Train Control, and other FRA Regulations as applicable. The Safety and Security Certification Program applies to all phases of the CHSTS, from preliminary engineering to the start of revenue operations, for each segment designed and built for the system. Federal Railroad Administration approval to operate will be achieved through final safety and security certification prior to the start of revenue service.

The Safety and Security Certification Program (SSCP) comprises verification and validation processes and principles consistent with the program-level *Verification and Validation Management Plan* (VVMP). The SSCP scope encompasses safety and security certification of the facilities, systems and equipment, safety-related procedures, training programs, and hazard and vulnerability resolution activities and operational readiness for the project. The process can be categorized into distinct progress factors throughout the advancement of the project. Specifically, safety and security certification focuses on the following certifiable factors:

- Hazard and Vulnerability Resolution Conformance
- Design Criteria Conformance
- Construction Specification Conformance
- Safety-Related Testing Conformance
- Operations and Maintenance Manuals Conformance
- Rules and Procedures Conformance
- Training Conformance
- Emergency Drills Conformance
- Integration Testing and Start-up

Certification will be performed in phases, both geographically and chronically, by contract package once the Project moves beyond the Preliminary Engineering Phase. Certification of latter-phase contract packages may consist of one or more certifiable elements defined in Section 7.4.1. The exceptions to this are the system wide activities such as procedures, training, emergency drills and integration testing and start-up which will be certified for the complete system.

Certification occurs at the beginning of each project phase, and is required for advancing system elements into the next phase. For example, the Final Design of a bridge structure must be certified to meet all safety and security design criteria prior to construction, and then must be certified to have been built in conformance to those safety and security design criteria before being placed into operation. This process assures the Authority that CHSTS elements are safe and secure as they move through each successive phase of the System development.

Certification Items that are not completed prior to moving to the next phase are placed on an Open Items List and tracked to completion. The Open Items List describes a plan for closure of the Certifiable Items, including target dates and an accountable person for closure.

After completion of each certifiable element a Certificate of Conformance (COC) is issued. The COC required for the various components necessitate the performance of a variety of system safety, security, and fire/life safety activities. The activities may be performed either independently, or integrated with other tasks such as acceptance testing or quality control measures. Regardless of whether the activities

are performed independently or integrated with others, adequate system safety, security, and fire/life safety activity records must be developed and maintained as evidentiary support for the COC.

The verification and validation (V&V) process defined in VVMP will be used to implement and monitor the certification process. Generally safety V&V methodology is comprised of conformance with the design criteria and collection of drawings, analyses, tests, calculations, observation, measurements, etc., performed at different stages in system development to demonstrate compliance with all safety requirements. Verification and Validation activities involve a number of analyses such as hazard analyses, operational analysis, and risk analyses; data collection; performance evaluation; field measurements; and product refinement including subsystem testing, field testing, integration testing and revenue service testing.

The PMT, led by the PMT Safety Manager will develop a Certifiable Elements and Hazards Log (CEHL) for safety-critical and security-critical system elements and their associated hazards and the mitigations developed during the hazard analysis process. The CEHL will carry though all of the project phases to ensure that hazards identified in the Preliminary Engineering Phase are mitigated consistently throughout the project life cycle. The Final Design and Construction Contractors shall update and revise the CEHL according to their project scope, with conformance to the Program-level CEHL as a requirement.

Mitigations will provide input to the design criteria in the form of requirements. The design criteria will then be examined for all safety-critical items that must be certified, resulting in Certifiable Items Lists that include all mitigations from the hazard analysis plus other identified safety-critical items. Certifiable Items Lists for each project phase lead in turn to development of Certifiable Items Lists for the subsequent project phase.

Certifiable Items Lists that are specific to safety and security requirements will be distinctly identified as such and tracked in conformance with the VVMP, and collectively make up the verification and validation evidence that supports safety and security certification.

7.2 Program Goals and Objectives

The goals of the Safety and Security Certification Program are to verify that identified safety and security requirements have been met in the preliminary engineering, final design, and construction phases and to provide evidence that the CHSTS is safe and secure for revenue service. The objectives of the Safety and Security Certification Program are to document the following:

- Safety and security design criteria are reflected in contract documents
- Facilities and equipment have been designed, constructed, manufactured, inspected, installed, and tested in accordance with safety and security requirements
- Operations and maintenance procedures and rules have been developed and implemented to ensure safe operations
- Training documents have been developed for the training of operating and emergency response personnel
- Transportation and maintenance personnel have been trained and qualified
- Emergency response agency personnel have been prepared to respond to emergency situations in or along the CHSTS corridor
- Safety and security systems integration tests have been conducted
- All safety and security related issues have been addressed and resolved

7.3 Responsibilities

The Authority Safety and Security Manager, with the assistance of the PMT System Safety Manager and PMT System Security Manager, will have overall responsibility for the administration of the Safety and Security Certification Program.

Safety and security certification is managed by the Authority Safety and Security Manager through the oversight and approval of the SSPC.

The SSPC will be responsible for tracking the progress of safety and security certification through regular review and update of the CEHL maintained by the PMT Safety Manager and PMT Security Manager.

Federal Railroad Administration approval to operate will be achieved through final safety and security certification prior to the start of revenue service.

7.4 Safety and Security Certification Process

The CHSTS safety and security certification process will follow the methodology defined in detail in VVMP. The certification process will be divided in the following distinct stages and steps.

- Stage 1: Environmental Review / Preliminary Engineering
- Stage 2: Design / Build Contracts
  - Step 1: Final Design
  - Step 2: Construction
  - Step 3: Testing / Acceptance
- Stage 3: Final Integration, Testing and Certification

During the preliminary engineering phase Preliminary Hazard Analysis (PHA), Site-specific Hazard Analysis (SiSHA) will be performed by the PMT System Safety Manager. Hazards are identified by various means such as historical data, generic hazard checklists, conceptual design, already developed design criteria, scenario development and the subjective judgment of a hazard management team during formal brainstorming workshop sessions. The hazard analysis is then performed on the identified hazards. The principal means of identifying security-related design criteria are Threat and Vulnerability Assessments (TVA) conducted by the PMT System Security Manager in collaboration with the other PMT discipline technical experts. Other analyses are conducted as necessary. The adopted mitigation measures from the PHA and TVA could provide input to design criteria or can be tracked on the CEHL and CETVL. The mitigation measures identified in SiSHA are contract specific and are tracked for resolution in the specific Design/Build (D/B) contract.

Each D/B contract will be certified in three steps as defined in VVMP. Once all design/build contracts have been successfully completed and certified, the CHSTS as a whole system will be integrated, tested and certified under supervision of the Authority.

7.4.1 Certifiable Elements

The Project has defined eight major CHSTS components for safety and security certification. They are referred to as the “Certifiable Elements”. Some or all of the nine certifiable factors identified in Section 7.1 will apply to each of the following eight “Certifiable Elements”. Samples of sub-elements are listed under the Certifiable Elements.

- Trainway
  - Track
  - Structures
  - Tunnel
  - Alignment
  - Access/egress facilities
- Station(s)
  - Escalators
  - Elevators
  - Station structure

  - Stand-by generators
  - Platform
  - Concourse
- Support Facilities
  - Storage/setup Yards
  - Vehicle Maintenance Facilities
  - Track maintenance facilities
  - Operations Control Center
- Traction Power
  - Traction Power Substations
  - Switching Stations
  - OCS
- Ventilation
  - Emergency Ventilation System
  - Ventilation Structure
- Train Control
  - Automatic Train Protection
- Communications
  - Radio
  - Closed Circuit TV
  - Emergency Telephone
  - Emergency Trip Station
  - Fire Telephone
  - Public Address System
- Utilities
  - HST Power Facilities
  - HST Fuel Lines
  - HST Water/Sewer
  - HST Communications
  - Non-HST Power
  - Non-HST HazMat Pipes
  - Non-HST Carrier Pipes non-HazMat
  - Non-HST Water/Sewer

The sub-element listing will be modified and expanded as project develop, as additional hazard analyses are performed, and as new or modified hazards are identified. Hazard identification can be performed by the Authority, the PMT, or Design/Build Contractors but all hazards must be tracked through the one central CHSTS CEHL.

7.4.2 Tracking of Hazards and Vulnerabilities

A *Certifiable Elements and Hazards Log* will be established during the Preliminary Engineering Phase. The CEHL identifies the major elements of the CHSTS that are to be proven to be safe prior to the startup of revenue service and acts as a guide for the certification process throughout project life cycle. Hazards associated with each major element that can reasonably be expected to occur in the CHSTS will be identified through a Hazard Analysis process and placed on the CEHL. The CEHL will be developed by the PMT System Safety Manager in collaboration with the other PMT discipline technical experts and

presented to the SSPC for review. The CEHL will be updated and expanded following the completion of analyses during the various phases of the CHSTS. A sample CEHL is depicted in Figure 7-1. Regular updates of the log will be presented to the SSPC and included in the quarterly reports to the SSEC.

For security certification a *Certifiable Elements and Threats and Vulnerabilities Log* (CETVL) will be established during the Preliminary Engineering Phase. The CETVL identifies the major elements of the CHSTS that are to be proven to be secure prior to the startup of revenue service and acts as a guide for the certification process throughout project life cycle. The CETVL will be developed by the PMT System Security Manager in collaboration with the other PMT discipline technical experts and presented to the SSPC for review and approval. The CETVL will be updated and expanded following the completion of security analyses during the various phases of the CHSTS. The CETVL format will be similar to CEHL.

Figure 7-1 CEHL (Sample)

California High-Speed Rail Program
Certifiable Elements and Hazards Log
Monday, December 09, 2013

Absolute Number	Date Identified	Hazards & Mitigations/Critical Items	Certified for Preliminary Engineering	Date Certified for Preliminary Engineering	Certified for Final Design CP01	Date Certified for Final Design CP01	Certified for Construction CP01	Date Certified for Construction CP01
		locations.						
10	---	**1.1.1.7 High Winds** High winds						
154	8/30/2011	***1.1.1.7.1 Mitigation #1*** [1] SYS/O&M: Perform wind analysis for effects on vehicles and operations.						
155	8/30/2011	***1.1.1.7.2 Mitigation #2*** [2] SYS: Install weather stations at regular intervals to monitor wind conditions.						
156	8/30/2011	***1.1.1.7.3 Mitigation #3*** [3] O&M: Develop operational responses to extreme wind conditions.						
157	8/30/2011	***1.1.1.7.4 Mitigation #4*** [4] INF: Install wind barriers at high-risk locations where need is supported by wind analysis.	DCM [STR] 12.3 Types of Structures DCM [STR] 12.5.1.1 Dead Load (DC, DW) DCM [STR] 12.5.2.6 Wind Loads (WS, WL) DCM [STR] 12.8.6.17 Walkways, Parapets, and Sound Walls DD-ST-001 AERIAL STRUCTURE, TWO TRACK NON-BALLASTED, TYPICAL CONFIGURATION ON TOP OF DECK DD-ST-002 AERIAL STRUCTURE, ONE TRACK NON-BALLASTED, TYPICAL CONFIGURATION ON TOP OF DECK DD-ST-020 AERIAL STRUCTURE, SOUND WALL CONFIGURATION DD-ST-021 EMBANKMENT, SOUND WALL CONFIGURATION					
12	---	**1.1.2 Collision**						
21	---	**1.1.2.1 Collision between HSR trains**						
161	8/30/2011	***1.1.2.1.1 Mitigation #1*** [1] INF: Track center spacing exceeds the combined dynamic envelopes of the trains.	DCM [CLR] 3.5 Track Center Spacing	5/9/13				
162	8/30/2011	***1.1.2.1.2 Mitigation #2*** [2] SYS:						

Page 22 of 95 Created by: IBM Rational DOORS 9.3

Note – Figure 7-1 is a sample representation only. Refer to current CEHL for identified hazards and required mitigations.

7.4.3 Certifiable Items Lists

The Design Criteria Manual establishes criteria, guidelines and requirements for the design of Infrastructure and Systems elements of the CHSTS. These criteria include design survey and mapping, trackway clearances, track geometry, trackwork, rolling stock and vehicle intrusion protection, civil, drainage, utilities, geotechnical, seismic, structures, tunnels, stations, support facilities, facility power and lighting systems, traction power supply systems, overhead contact system and traction power return system, grounding and bonding requirements, corrosion control, automatic train control, yard signaling, electromagnetic compatibility and interface, supervisory control and data acquisition subsystems,

communications, rolling stock core systems interfaces, and safety and security. The design criteria shall be reviewed by the PMT System Safety Manager for safety-critical items that must be certified, whether or not they were developed as a result of the hazard analysis activities. All safety-critical items will be added to a Certifiable Items List and verified in conformance with the V&V process identified in the VVMP.

V&V Certifiable Items Lists for each project phase lead in turn to development of V&V Certifiable Items Lists for the subsequent project phase.

7.4.4 Verification and Validation of Final Design and Construction

Design Criteria are requirements for the Final Design. The verification and validation process, as identified in the *CHSTS Verification and Validation Management Plan*, shall be utilized for verifying that the identified mitigations have been satisfactorily incorporated into the Final Design.

The Design/Build Contractors shall be responsible for completing the Certifiable Items Lists applicable to their specific project scope during the Final Design Phase. The Design/Build Contractors shall identify in the resolution section of the Certifiable Items Lists objective evidence that demonstrates compliance with the required safety-critical or security-critical design criteria. Requests for variance from the requirements identified in the Certifiable Items Lists shall be handled through the process identified in Section 5.4.

All completed Certifiable Items Lists, along with associated supporting material, shall be compiled by the Design/Build Contractors and available for audit by the Authority Safety and Security Manager upon request. When all Certifiable Items Lists for a particular element or infrastructure component are completed, a Final Design Certificate of Conformance Package consisting of a Certificate of Conformance for the project element, all completed Certifiable Items Lists, and all supporting documentation such as hazard analysis, drawings, and design element descriptions shall be compiled.

The Certifiable Items Lists shall be expanded by the Design/Build Contractors to include a Construction section upon completion of the Final Design phase of a particular CHSTS element. The safety- and security-critical items identified during the Final Design Phase shall be carried over into the Construction Phase.

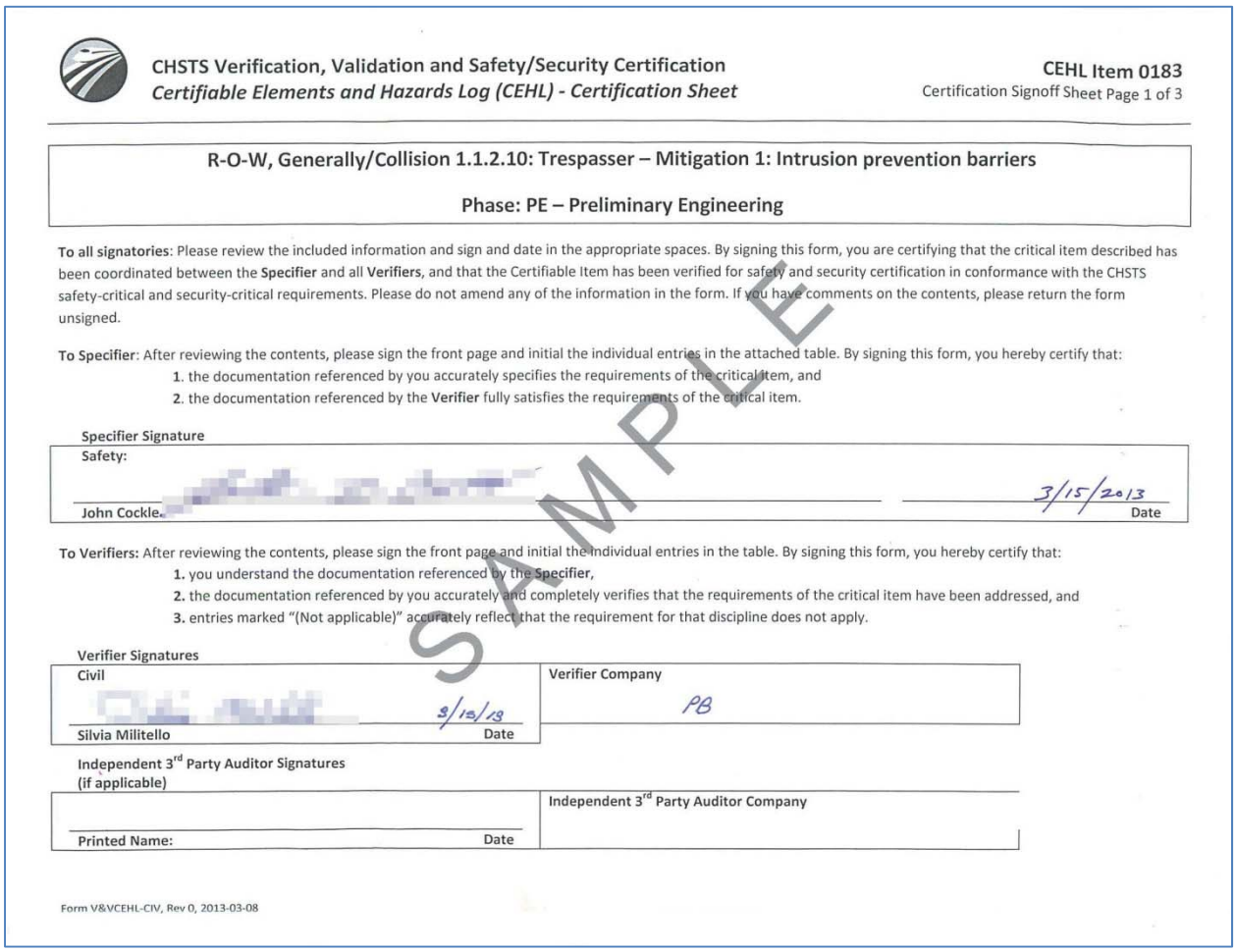
The Design/Build Contractors shall be responsible for completing the Certifiable Items Lists that apply to their scope of work during the Construction Phase. The Design/Build Contractors shall identify in the resolution section of the Certifiable Items Lists objective evidence that demonstrates compliance with design features that are identified as safety-critical or security-critical. Requests for variance from the requirements identified in the Certifiable Items Lists shall be handled through the process identified in Section 5.4.

All completed Certifiable Items Lists, along with associated supporting material, shall be compiled by the design/build contractors and available for audit by the Authority Safety and Security Manager upon request. When all Certifiable Items Lists for a particular element or infrastructure component are completed, a Construction Certificate of Conformance Package consisting of a Certificate of Conformance for the project element, all completed Certifiable Items Lists, and all supporting documentation such as hazard analysis, field reports, photographs, and drawings shall be compiled.

All completed Certificate of Conformance Packages (Final Design or Construction) shall be submitted to the Authority through the SSPC for review and a Statement of No Objection (SONO), and eventual review and acceptance by the Authority through the SSEC.

A sample Certificate of Conformance is depicted on Figure 7-2.

Figure 7-2 Certificate of Conformance (Sample)



CHSTS Verification, Validation and Safety/Security Certification
Certifiable Elements and Hazards Log (CEHL) - Certification Sheet

CEHL Item 0183
Certification Signoff Sheet Page 1 of 3

R-O-W, Generally/Collision 1.1.2.10: Trespasser – Mitigation 1: Intrusion prevention barriers

Phase: PE – Preliminary Engineering

To all signatories: Please review the included information and sign and date in the appropriate spaces. By signing this form, you are certifying that the critical item described has been coordinated between the **Specifier** and all **Verifiers**, and that the Certifiable Item has been verified for safety and security certification in conformance with the CHSTS safety-critical and security-critical requirements. Please do not amend any of the information in the form. If you have comments on the contents, please return the form unsigned.

To Specifier: After reviewing the contents, please sign the front page and initial the individual entries in the attached table. By signing this form, you hereby certify that:

1. the documentation referenced by you accurately specifies the requirements of the critical item, and
2. the documentation referenced by the **Verifier** fully satisfies the requirements of the critical item.

Specifier Signature
Safety:
John Cockle. 3/15/2013 Date

To Verifiers: After reviewing the contents, please sign the front page and initial the individual entries in the table. By signing this form, you hereby certify that:

1. you understand the documentation referenced by the **Specifier**,
2. the documentation referenced by you accurately and completely verifies that the requirements of the critical item have been addressed, and
3. entries marked "(Not applicable)" accurately reflect that the requirement for that discipline does not apply.

Verifier Signatures
Civil
Silvia Militello 9/12/13 Date
Verifier Company PB

Independent 3rd Party Auditor Signatures (if applicable)
Printed Name: Date
Independent 3rd Party Auditor Company

Form V&VCEHL-CIV, Rev 0, 2013-03-08

SAMPLE

7.4.5 Testing Verification

The Certifiable Items Lists shall be expanded to include a Testing section upon completion of the Final Design phase of a particular CHSTS element. The safety- and security-critical items for systems identified during the Final Design and Construction Phases shall be carried over into the Testing Phase. In addition, the relationships between systems and subsystems shall be analyzed for systems integration requirements as identified in a Systems Integration Test Plan, and Certifiable Items Lists for integrated testing shall be developed to prove the integration of associated systems.

The Systems Contractor(s) shall be responsible for any additional analyses that are required (PHA, TVA, FMEA, IHA, SHEA, FTAn and OHA as appropriate), as the safety-critical or security-critical testing criteria are developed and applied to specific CHSTS or subsystem elements. The systems contractor(s) shall be responsible for developing and completing the Certifiable Items Lists that apply to their scope of work during the Testing Phase. The system(s) contractor must identify in the resolution section of the Certifiable Items Lists objective evidence that demonstrates compliance with testing requirements that are identified as safety-critical or security-critical. Requests for variance from the requirements identified in the Certifiable Items Lists shall be handled through the process identified in Section 5.4.

All completed Certifiable Items Lists for system testing or system integration, along with associated supporting material, shall be compiled by the systems contractor(s) and available for audit by the Authority Safety and Security Manager upon request. When all Certifiable Items Lists for a particular system element or integrated system relationship are completed, a Testing Certificate of Conformance Package (consisting of a Certificate of Conformance for the required system tests, all completed

Verification Checklists, and all supporting documentation such as hazard analysis, field reports, photographs, and drawings) shall be compiled and forwarded to the PMT System Safety Manager. The PMT System Safety Manager shall review the Testing Certificate of Conformance Package for completeness and content accuracy, and shall then forward the Testing Certificate of Conformance Package to the Authority through the SSPC for review and SONO, and eventual review and acceptance by the Authority through the SSEC.

7.4.6 Startup Verification

The Certifiable Items Lists shall be expanded by the PMT System Safety Manager to include a Startup section as the CHSTS is prepared for the start of revenue operations. The safety- and security-critical items for operational readiness of the CHSTS identified during the Final Design, Construction and Testing Phases shall be carried over into Startup. Certifiable startup items include but are not limited to operation plans, emergency preparedness plans, training programs, timetables and rulebooks.

The O&M contractor(s) shall be responsible for completing the Certifiable Items Lists that apply to their scope of work prior to Startup. The O&M contractor(s) must identify in the resolution section of the Verification Checklists objective evidence that demonstrates compliance with requirements for the start of revenue operations that are identified as safety-critical or security-critical. The O&M contractor(s) shall be responsible for any additional analyses that are required (PHA, TVA, FMEA, IHA, SHEA, FTAn and OHA as appropriate), as the safety-critical or security-critical criteria for startup are applied to specific CHSTS, subsystem or operational elements. Requests for variance from the requirements identified in the Certifiable Items Lists shall be handled through the process identified in Section 5.4.

All completed Certifiable Items Lists for the start of revenue operations, along with associated supporting material, shall be compiled by the O&M Contractor(s) and available for audit by the Authority Safety and Security Manager upon request. When all Certifiable Items Lists for a particular system or operational element are completed, a Startup Certificate of Conformance Package (consisting of a Certificate of Conformance for the startup requirements, all completed Certifiable Items Lists, and all supporting documentation such as hazard analysis, field reports, photographs, and drawings) shall be compiled and forwarded to the PMT System Safety Manager. The PMT System Safety Manager shall review the Startup Certificate of Conformance Package for completeness and content accuracy, and shall then forward the Startup Certificate of Conformance Package to the SSPC for review and SONO, and eventual review and acceptance by the Authority through the SSEC.

7.4.7 Open Items List

Certifiable Items that cannot be closed prior to the start of the next project phase shall be placed on an Open Items List for tracking purposes. The Open Items List shall describe the Certifiable Item itself, restrictions or conditions that permit the movement of the project element to the next project phase, a target date for closure, and a person of accountability for the certifiable item. The Open Items List shall be maintained by the Authority Safety and Security Manager and periodically reviewed by the SSPC for progress and completeness.

7.4.8 Conditional Use Permit

Certifiable Items that require placement on the Open Items List shall be reviewed by the Authority Safety and Security Manager and additional hazard analysis applied as appropriate. The results of the hazard analysis shall be incorporated into a Conditional Use permit that describe the conditions or restrictions that allow the use or advancement of the certifiable item into the next project phase before certification for that item is complete. The Conditional Use Permit shall be presented to the SSPC for review and SONO. The Conditional Use Permit shall describe all conditions or restrictions associated with the conditional use of the Certifiable Item, including an expiration date. Revisions to the Conditional Use Permit, including extension of the expiration date, shall require further review and SONO by the SSPC.

8.0 CONSTRUCTION SAFETY AND SECURITY

8.1 Overview

The purpose of the construction safety and security program is to define the minimum health, safety and security requirements to which all participating CHSTS staff, Contractors and subcontractors shall adhere to in fulfilling the Authority's commitment to ensuring a safe and secure construction project. This commitment includes the prevention of job-related injuries and illnesses for the workers engaged in project construction activities, as well as providing safe and secure conditions during construction of the project for the members of the public, who live, work or travel near to the project work areas.

All applicable codes and regulations must be followed by employees engaged in construction activities, including but not limited to the following:

- California Code of Regulations Title 8 Construction Safety Orders
- Federal Railroad Administration regulations as found at 49 CFR 214, 49 CFR 219, 49CFR225, 49 CFR 228, 49 CFR 236
- CPUC General Orders
- Other applicable federal and state OSHA regulations

Contractors shall be required to develop a program-level Safety and Security Management Plan (SSMP) specific to their scope of work, as well as Site-Specific Health and Safety Plans (SSHASP) and a Site-Specific Security Plans (SSSP) that identify the local conditions and requirements peculiar to the site and work to be performed, in compliance with the above regulations.

Contractors are responsible for ensuring the compliance of their employees and subcontractor's with their SSMP, SSHASP and SSSP.

8.2 Program Elements

The Contractor shall be responsible for all aspects of safety and security at the project work site, as required through the standard contract provisions. The *CHSTS Construction Safety and Security Program* (Appendix B) describes the basic programmatic requirements for construction safety and security, compliance to which is required through the CHSTS construction contract documents.

8.2.1 Safety and Security Management Plan

The Contractor's SSMP will identify the qualification and organizational structure of the Safety and Security Team, and the processes that the Contractor will employ to manage the SSHASP(s) and SSSP(s). Principle elements of the Contractor's SSMP will include hazard management, security management (threats and vulnerabilities), a program for ensuring compliance to the Contractor's SSMP, training, communication, coordination with adjacent third-party requirements (including adjacent railroads and roadways), emergency response plans and procedures, hazardous materials handling and communications, public safety, and other safety and security elements as identified in the Contractor's corporate safety and security program.

The SSMP will be submitted to the Authority for review and Statement of No Objection (SONO).

8.2.2 Site-Specific Plans

The Contractor will be required to develop and implement SSHASPs and SSSPs specific to its contract scope of work on the CHSTS, in conformance with the *CHSTS Construction Safety and Security Program* contract requirements. A site-specific Job Hazard Assessment (JHA) and TVA will be performed by the Contractor to determine the safety processes, equipment utilized, and personnel assignments to be provided by the Contractor at each project work site.

8.2.3 Construction Safety and Security Management

The PMT Construction Safety Manager and Project Construction Management team will be responsible for the management oversight of the entire construction safety and security program. The PMT Construction Safety Manager and Project Construction Management team will verify contractor compliance with the safety and security requirements of the approved SSMP, SSHASPs, SSSPs, and other safety/security related contract provisions and applicable regulations throughout the construction, testing and start-up phases of the CHSTS. The PMT Construction Safety Manager and Project Construction Management team will audit Contractor activities and results will be reported to the Authority's Safety and Security Manager.

8.2.4 Stop Work Order

The CHSTS construction management plan will establish procedures regarding control of nonconforming work and stop work orders. In the event that a failure to meet safety and/or security requirements results in imminent danger to workers or the general public or property, a Stop Work Order will be issued by the CHSTS Construction Manager.

The CHSTS stop-work procedure shall apply to all construction activities. The stop-work procedure will be used only where imminent danger situations exist. An "imminent danger" is any condition or practice that could reasonably be expected to cause death or serious physical harm immediately or before the danger can be eliminated by normal means.

Stop-work orders will be in effect until the issuing authority determines that the problem(s) is resolved and the work area(s) is brought to satisfactory conformance with health, safety and security requirements.

8.3 Construction Risk Management

The CHSTS is committed to identifying and managing construction safety hazards and security vulnerabilities as subdivisions within the general issue of project risk. Risk in this context includes those events that, if they do occur, could impact safety, security, the environment, CHSP System's interests or the interests of third parties, including property owners and municipalities.

Risk Management is utilized by the CHSTS as a decision support tool, specifically identifying areas of high risks, which are reviewed to ensure that all reasonable practicable measures are taken to mitigate them. Risk Control measures shall be identified for all risks to the System. These include financial and schedule risks as well as property, safety and security risks.

For the construction phase, prior to finalization of the contract documents, surveys to identify any unique hazards, threats, or vulnerabilities that may exist for the particular construction elements will be conducted and actions to mitigate these hazards or vulnerabilities will be included in the Special Provisions of the specific contract package.

During construction, each contractor shall cooperate with CHSTS staff and other interested parties in providing information needed in connection with risk management of its contract works. The contractor will prepare and submit to the PMT Risk Manager a Risk Management Plan for review and acceptance. The Risk Management Plan shall be based upon the CHSTS *Program Risk Management Plan* and shall include a means of monitoring progress in the reduction of the overall number and impact of risks through the use of a Risk Register which shall be in a format acceptable to the PMT Risk Manager. Safety hazards and security vulnerabilities shall be identified as risks, and will be included as special categories in the Risk Register.

During the contract each contractor's Risk Register shall be updated monthly and submitted to the PMT in hard copy and electronic formats. The risks identified by the contractor shall be integrated into the CHSTS Risk Register.

The Contractor's Risk Management process shall ensure that as far as is reasonably practicable:

- All risks are identified;

- Judgments are made as to risk importance;
- Risk exposure is reduced to acceptable levels;
- Risk control measures are assessed against cost benefit as appropriate; and
- Control measures are reviewed and managed until close out.

For the top “critical” risks from the Risk Register each contractor shall provide a narrative for each Critical risk identified in this category section and the mitigation plan proposed. Safety hazards and security vulnerabilities will be treated as separate categories of risk, and will be classified as Critical depending on specific site conditions.

9.0 STATE SAFETY OVERSIGHT REGULATIONS

9.1 Applicability

The California High-Speed Train System does not fall under the Federal Transit Administration applicability regulations for State Safety Oversight, described in 49 CFR 659. As such, this section does not apply. The Federal Railroad Administration has authority for oversight of safety regulations.

10.0 COORDINATION WITH FEDERAL RAILROAD ADMINISTRATION

10.1 Activities

The California High-Speed Train System will design and construct a railroad system that is regulated by the Federal Railroad Administration. FRA regulation is by directive under the United States Department of Transportation.

Effective on the date the railroad begins revenue operations, the following generally applicable federal railroad safety regulations from Title 49, Code of Federal Regulations, and any amendments thereto are made applicable to the CHSTS, except where the CHSTS is granted relief through an FRA waiver.

- Part 207, Railroad Police Officers
- Part 209, Railroad Safety Enforcement Procedures
- Part 210, Railroad Noise Emission Compliance Regulations
- Part 211, Rules of Practice
- Part 212, State Safety Participation Regulations
- Part 213, Track Safety Standards
- Part 214, Railroad Workplace Safety
- Part 215, Freight Car Safety Standards
- Part 216, Special Notice and Emergency Order Procedures
- Part 217, Railroad Operating Rules
- Part 218, Railroad Operating Practices
- Part 219, Control of Alcohol and Drug Use
- Part 220, Railroad Communications
- Part 221, Rear End Marking Device
- Part 222, Use of Locomotive Horns at Public highway-Rail Grade Crossings
- Part 225, Railroad Accidents / Incidents: Reports, Classification and Investigations
- Part 227, Occupational Noise Exposure
- Part 228, Hours of Service of Railroad Employees
- Part 229, Railroad Locomotive Safety Standards
- Part 231, Railroad Safety Appliance Standards
- Part 232, Brake System Safety Standards
- Part 233, Signal Systems Reporting Requirements
- Part 235, Instructions Governing Applications for Approval of a Discontinuance
- Part 236, Rules, Standards and Instructions Governing the Installation, Inspection, Maintenance and Repair of Signal and Train Control Systems, Devices, and Appliances
- Part 237, Bridge Safety Standards
- Part 238, Passenger Equipment Safety Standards
- Part 239, Passenger Train Emergency Preparedness
- Part 240, Qualification and Certification of Locomotive Engineers
- Part 242, Passenger Train System Safety Plans
- Part 270, System Safety Program (under development)

The CHSTS will submit to the FRA any plans, programs, and procedures that affect the safe operation of the system, or which are required to demonstrate compliance with the applicable regulations.

Throughout Preliminary Engineering and Final Design phases the CHSTS will communicate with the FRA to ensure that the FRA is current on the status of operations and engineering design requirements as they are developed. CHSTS will maintain regular contact with FRA during development of operating rules, training of maintenance and operating personnel and development of operating practices prior to the start of revenue service.

As detailed in Section 7.0 of this SSMP, the CHSTS will manage a safety and security certification program to record and demonstrate that all safety and security requirements for the project are identified and integrated into the final system.

10.2 Implementation

The CHSTS, through the Program Management Team, will maintain communications with the FRA representatives throughout the Planning, Preliminary Engineering, Final Design, Construction, and Testing and Start-up phases.

10.3 Coordination Process

Interface and coordination with FRA will be conducted through the PMT. The PMT will designate those persons authorized to interface with agents of the FRA to ensure that information and decisions communicated between CHSTS and FRA are consistent, correct and authorized.

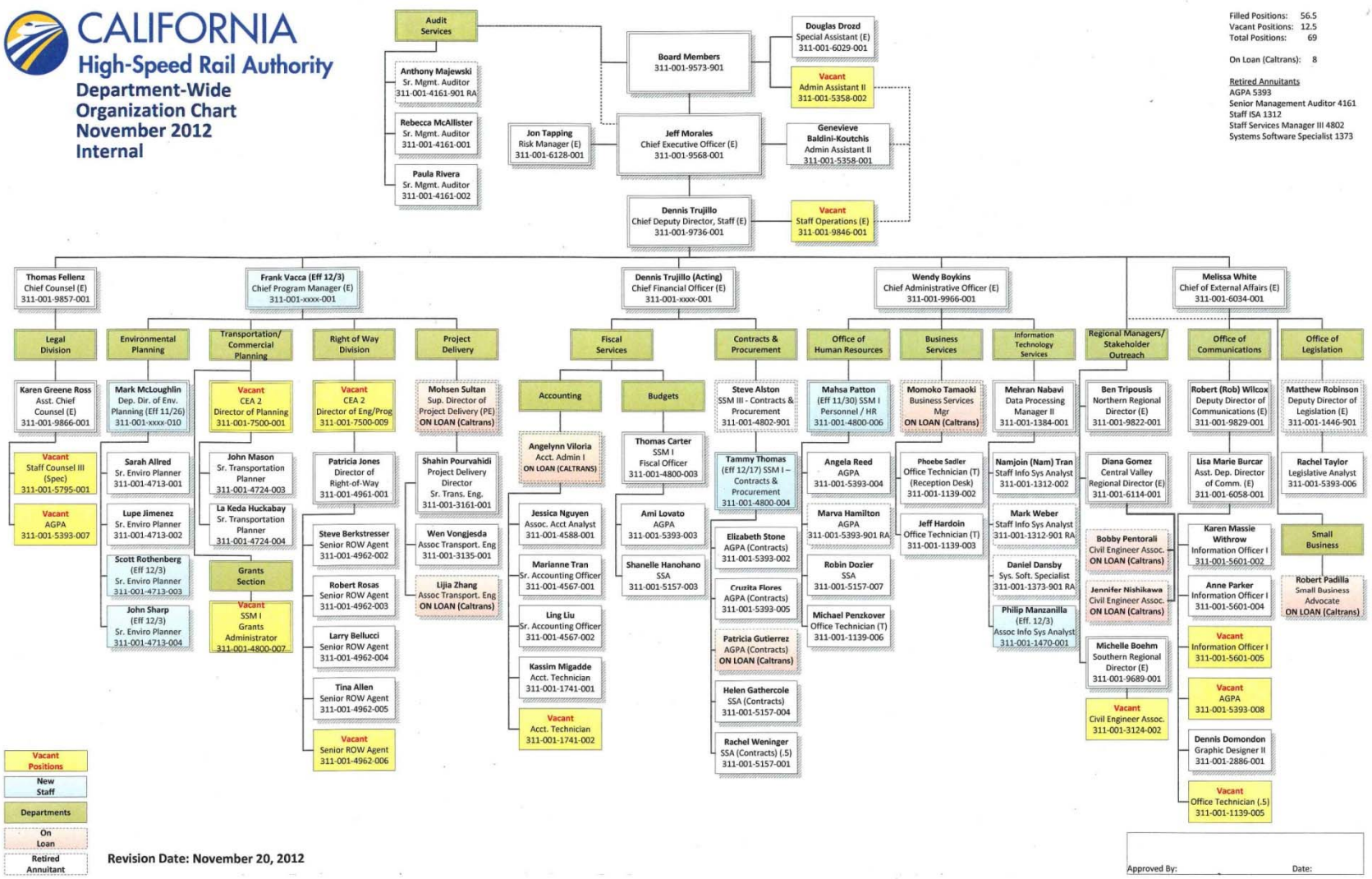
The FRA will provide guidance to the PMT with regard to applicable regulations, documents that will require formal submission and approval, and how any variances may be processed.

11.0 DEPARTMENT OF HOMELAND SECURITY COORDINATION

There are currently no DHS requirements or security directives that have been issued by the Transportation Security Administration (TSA) applicable to new builds, and particularly high-speed rail. The Authority will develop a System Security Program Plan (SSecPP) prior to revenue operation. The SSecPP will fulfill DHS/TSA requirements for an operating railroad, which include development of an SSecPP, and designating a primary and alternate Security Coordinator and providing TSA with names and contact information for 24 hour/7 days per week availability. The Security Coordinator will have a direct reporting relationship to the Authority Chief Executive Officer regarding matters of security.

The Authority has established liaison with the TSA Mass Transit and Rail Department through the PMT System Security Manager who reports directly to the project operations manager. This liaison has been established to ensure all DHS/TSA requirements will be met once the project is complete, and to stay current with all security concerns, threats, best practices and developing security regulations that affect rail security.

APPENDIX A – CALIFORNIA HIGH-SPEED RAIL AUTHORITY ORGANIZATIONAL CHART



APPENDIX B – CHSTS CONSTRUCTION SAFETY PROGRAM REQUIREMENTS

1.0 CHSTS CONSTRUCTION SAFETY AND SECURITY PROGRAM

1.1 Safety and Security Program Objectives

The Safety and Security Program objectives are as follows:

a. Prevent personal injuries and property damage or loss;

b. Provide safe and secure work environment for employees, contractors, passengers, emergency responders, third parties, and the public at large;

c. To convey the CHSRP Safety and Security Policy Statement to all contractors and subcontractors;

d. To ensure compliance with the stated objectives and requirements contained in the CHSRP Safety and Security Policy Statement, the Contractor's SSHASP, the Contractor's SSSP, Contract provisions, applicable Laws, and industry consensus standards;

e. To identify general requirements for the Contractors' workplace safety and security programs; and

f. To identify a process for the Authority approval of the safety and security submittals.

1.2 Construction Safety and Security

1.2.1 Contractor Responsibilities

The Contractor is responsible for ensuring safety and security at all of its work sites, including the activities of Subcontractors. Safety and security management and enforcement for each contract shall be administered by employees (direct hire) of the Contractor. This responsibility shall not be delegated nor contracted out to Subcontractors, suppliers, consultant service/company, or any other persons/agency without written approval from the Authority. The effectiveness of the Contractor's safety and security efforts depends upon active participation, cooperation, and compliance by the Contractor's and Subcontractors' project managers, superintendents, supervisors, and other employees.

The Contractor shall:

a. Plan and execute all Work to prevent personal injury and property damage or loss, and ensure public safety, security of all people and assets;

b. Comply with Laws, applicable industry consensus standards; and the Authority and Contractor policies, procedures, and requirements;

c. Define, implement, and maintain a program for prompt identification and correction of hazards and unhealthy practices and conditions;

d. Define, implement, and maintain a program for prompt notification and investigation of all incidents of injury, damage, or near-miss incidents to determine causes and take necessary corrective action to prevent re-occurrence;

e. Define, implement and maintain a system of prompt identification, notification, investigation, and correction of security breaches and incidents;

f. Develop, establish, and conduct a safety and security training program for all employees assigned to the Project;

g. Ensure proper tools, equipment, and processes are available for use as required for the work at hand, and are used according to the manufacturer's guidelines;

h. Maintain an accurate record of data utilizing the Authority's integrated Safety Management System for all identified hazards, near-misses, and accidents and incidents resulting in death, personal injury, occupational disease, or damage or loss to property, materials, supplies, or equipment;

i. Plan and execute all Work in compliance with the stated objectives and requirements contained in the CHSRP Safety and Security Policy Statement (contained in the CHSRP SSMP in Book IV, Part D.5); the Contractor's SSHASP and SSSP; Contract provisions; applicable federal, State, and local laws and regulations; and industry consensus standards;

j. Ensure all Subcontractors, suppliers, etc. are provided with a copy of the CHSRP Safety and Security Policy Statement, and the Contractor's SSHASP and SSSP, and are properly informed of their obligations with regards to compliance;

k. Complete safety and security certification requirements as identified in Section 1.2.1;

l. Obtain permits required by the California Division of Occupational Safety. Permits shall be kept on file at the Site;

m. Designate a Safety and Security Manager responsible to ensure the proper implementation of the SSHASP and SSSP and a team of Field Safety Representatives appropriate to the scope of the Project and work to be performed. The Contractor shall demonstrate that their representatives have sufficient knowledge and experience to perform the required duties;

   i. Minimum qualifications for the Safety and Security Manager include:

      - Ten years of heavy civil construction safety experience;
      - Certification as a Construction Health and Safety Technician, Certified Safety Professional, or Certified Safety/Security Director - Rail;
      - OSHA 30-hour Construction Training card; and
      - One year of FRA Roadway Worker Protection qualification per 49 CFR Part 213;
      - The Contractor may propose combinations of the above qualifications that demonstrate sufficient competency for the Safety and Security Manager position;

   ii. Minimum qualifications for the Field Safety Representatives include:

      - Three years of heavy civil construction safety experience;
      - OSHA 30-hour Construction Training card; and
      - First Aid/CPR;

n. Define, implement, and maintain a SSMP for the administration of the SSHASP(s), SSSP(s), and the Safety and Security Team including roles/responsibilities, reporting, and work plan approach; and

o. Contractor shall develop a plan for the use of heavy equipment that, when used, might encroach or otherwise intrude into third party operating space (public or adjacent railway). The plan must address how third party approval for potential encroachment will be achieved and how any safety requirements by third party will be communicated to the operators and responsible parties of the heavy equipment. Third party approvals shall be made available to the Authority for review upon request.

1.2.2 Contractor Deliverables

The Contractor shall submit the following:

a. A SSMP in accordance with the "Safety and Security Management Plan" clause (Section 1.2.3);

b. A SSHASP(s) in accordance with the "Construction Site-Specific Health and Safety Plan Elements" clause (Section 1.2.4);

c. SSSP(s) in accordance with the "Site-Specific Security Plan Elements" clause (Section 1.2.5);

d. A Safety and Security Certification Plan in accordance with the "**Error! Reference source not found.**" clause (Section **Error! Reference source not found.**);

e. Site-Specific Hazard Analysis (SiSHA) Reports and Site-Specific Threat/Vulnerability Assessment (SiSTVA) Reports, and an updated Certifiable Elements and Hazards Log, in support of the Contractor's Safety and Security Certification Plan. A SONO of new or revised SiSHAs and SSTVAs is required prior to commencement of Construction phase activities;

f. A monthly report utilizing the Authority's Integrated Safety Management System of safety performance including a narrative summary of safety activities, hazard identification and mitigation, incidents of injury or property damage incurred, injury rates, incident investigation results, corrective action plans, reports of near-miss incidents, a summary of communication and training efforts, a summary of field audits/observations for safety, a summary of Job Hazard Analyses completed, and other activities as identified by the Contractor; and

g. A monthly report of security performance, including incidents of trespass or security breach, incident investigation results, corrective action plans, a narrative summary of security activities, and other items as identified by the Contractor. The report shall be submitted to the Authority by close of the 5th business day of the following month.

1.2.3 Safety and Security Management Plan

The Contractor shall submit a SSMP to the Authority for review and SONO within 60 days following NTP. The SSMP will identify the qualification and organizational structure of the Safety and Security Team, and the processes that the Team will employ to manage the SSHASP(s) and SSSP(s). The SSMP shall:

a. Describe a process for managing hazards or incident of injury or damage through identification, reporting, and correction or abatement or mitigation, including descriptions for processes and applicability of Job Hazard Analyses (JHA) for each job assignment within the scope of the contract for which a person may be exposed to incidents of injury or illness. JHAs previously performed by the Contractor will be acceptable for use in determining preventive measures if the scope and functionality of the jobs under review are justifiably the same. The previously-performed JHAs, however, must address the specific characteristics of each site and tasks performed within the Project scope. JHAs shall be kept on the Site and made available to the Authority upon request;

b. Describe procedures for work site safety audits and inspections, including assignment of responsibility, frequency, documentation method, and actions following various audit results;

c. Describe the program for Safety and Security Program training employees of the Contractor, Sub-contractors, the Authority, and other applicable third parties. The training program description shall include safety and security program training requirements and documentation including training curriculum, frequencies of and method of delivery for training, training records, a method for identifying and certifying qualified employees, and lists of qualified/competent persons for specific tasks;

d. Describe an employee communication program that identifies individual responsibilities for all employees, schedules for specific communication techniques, and a process for recording and tracking communication program performance. The employee communication program shall include job briefing procedures/requirements, HazComm, employee safety and security committees, Project safety and security committees, and notification process for employees and the Authority of incidents or hazards when identified;

e. Describe a process for identifying applicable health and safety rules and regulations applicable to the tasks to be performed on the Project, including all local, State, and federal occupational safety and health regulations, including but not limited to California Code of Regulations Title 8 Construction Safety Orders, FRA regulations 49 C.F.R. Parts 200-299, California MUTCD, the Contractor's corporate safety plan, and the CHSRP Safety and Security Policy Statement. Rules and procedures shall address Site-specific work activities and conditions including:

   i. Safeguards for the protection of all workers, pedestrians, and the public from excavations, construction equipment, obstructions, and other dangers. Safeguards may include fencing, adequate railings, guard rails, temporary walks, barricades, warning signs, directional signs, overhead protection, planking, decking, danger lights, and other suitable safeguards;
   ii. Personal protective equipment requirements for all work site hazards and conditions, including equipment issuance/availability procedures;
   iii. Mobile equipment operation procedures and training program, including qualification process and requirements, and performance observation/evaluation requirements;
   iv. Fall protection and scaffolding procedures, including minimum fall protection equipment requirements, a process for training workers, and performance observation/evaluation requirements;

v. Motor vehicle operation program, including rules and procedures for specific equipment to be used at the work site (including industrial lift trucks), operator screening and qualification process and requirements, and performance observation/evaluation requirements;
vi. Roadway worker protection (on-track safety) for the Authority ROW in compliance with FRA regulations contained in 49 C.F.R. Part 214;
vii. Hazardous Materials handling and storage plan specific to each work site, including a plan for cataloguing Material Safety Data Sheets and submitting same to the Authority, and for communicating Material Safety Data Sheet information to employees;
viii. Lockout/tagout programs for all applicable energy sources, including electrical, hydraulic, and kinetic; and
ix. Fire prevention and suppression, including procedures for identification of hazards that could lead to fire, procedures for local fire suppression and notification to authorities, inspection processes, and a detailed training and exercise program;

f. Identify, develop, and implement a program for coordinating roadway worker protection activities and compliance with adjacent railroads. All contractors working in the shared corridor will meet frequently with the responsible representatives of the operating railway and coordinate activities to minimize risks and hazards to Contractor personnel, and to avoid hazards or disruptions to the operation of the railway;

g. Describe a process for managing security of Authority properties within the Contractor's Scope of Work. Security program elements shall include at a minimum:

i. Identification of threats and vulnerabilities, reporting, and controls or mitigation. Include process description and applicability of Threat and Vulnerabilities Assessments (TVAs) for each job location within the scope of the contract. Process should include how the processes would adapt in the face of imminent threat or change of security conditions;
ii. Description of how the planned deployment of security measures such as fencing, guards, lighting will be evaluated for initial effectiveness;
iii. Description of an audit and inspection plan to review security measures and ensure that controls are being managed effectively; and
iv. Description of the internal and external (Authority and local law enforcement) reporting structure and process for security incidents, including thresholds for reporting including at a minimum:

- Description of a program for reporting Security incidents. Incident reports for graffiti, vandalism, and trespass to be submitted to the Authority within 48 hours. Incident reports for any significant damage or conditions observed, and any injuries to employees, subcontractors or others will be submitted to the Authority immediately. Security reports submitted weekly to include:, daily security logs noting deployment of security personnel, any significant weather conditions, site locations covered, incident notifications or threats, any noted security equipment conditions (cut fence, broken lights). Copies of an reports from local agencies who respond to incidents on the Authority's property under Contractor control;
- Description of how the background check process will appropriately screen for internal threats to the security of the project Include a description of any code of conduct and expectations for employee behavior, and procedures for internal and external notification when personnel security is violated;
- Description of how the access control to project sites will be applied to ensure the security and control of all project sites including procedures for authorizing new employees or visitors, and procedures for monitoring access control performance;
- Description of the security awareness employee training program, content and schedule including record keeping of training completion;
- Description of the process for ensuring all subcontractors on site adhere to the Contractor's SSMP requirements; and
- A process for recommending enhancements to the Authority's security elements;

h. Identify, develop, and implement an Emergency Response Plan for management of emergency situations associated with, but not limited to, the following: injury to an employee or member of the public; fire; flood; earthquake; property damage and damage to various utilities (such as, electrical, gas, sewage, water, telephone, or public roadways); public demonstrations; sabotage or threats of sabotage; other security incidents or threats, Hazardous Materials encountered; toxic spills; explosions; vehicular accidents; and confined space rescues. The Emergency Response Plan shall include the following items, at minimum:

   i. Identification of the person responsible for handling an emergency;
   ii. Establishment of teams for handling each type of emergency;
   iii. Identification of the person responsible for making emergency call (preferably the ranking Supervisor present);
   iv. The requirement to conspicuously post a list of emergency phone numbers, along with information to be transmitted. Include with the emergency phone numbers, the number of the Authority's representative to be contacted (request telephone number and name of the Authority contact person or persons);
   v. Site identification and signage for emergency responders;
   vi. Trench and confined space rescue plan or tunnel evacuation plan, as applicable;
   vii. The procedure for contacting the Authority Representative when an incident requiring emergency response occurs; and
   viii. Scene management for the emergency response including procedures for ensuring the safety of employees and emergency responders, safeguarding the scene from unwanted entry, and handling on-scene media;

i. Identify, develop, and implement a HAZWOPER Plan for the control of hazardous substances in compliance with California Code of Regulations, Title 8, Section 5192;

j. Identify, develop, and implement a program for ensuring public safety at work sites and avoiding damage to public property. The public shall be considered as any persons and property not employed or owned by the Contractor or its Subcontractors. The program shall address site-specific work activities and conditions including:

   i. Identification of potential hazards to the public;
   ii. Erection and proper upkeep at all times of all necessary safeguards for the protection of the public, including pedestrian and vehicle traffic, and the assignment of trained and competent flaggers whose sole duties shall consist of directing the movement of public traffic through or around the Work site;
   iii. Posting of signs warning against the hazards created by construction or warranty service activities;
   iv. Elimination of unnecessary noise, obstructions, and other annoyances to nearby residents and businesses;
   v. Procedures and competency training for employees assigned to public safety and public property protection; and
   vi. Designated work zones – Work outside of the designated work zones shall be performed only when specifically stated in writing from the Authority Representative;

k. Identify, develop, and implement a program for Temporary Traffic Control. Temporary Traffic Control Plans will be developed in compliance with the requirements of the current California MUTCD. The Contractor shall apply to the jurisdictional authority for approval of the plan and for a permit or permits to work in the public ROW. In cases where there is more than one jurisdictional authority, a separate Temporary Traffic Control Plan will be developed for each jurisdictional authority, as required. The Temporary Traffic Control Plan shall include:

   i. Drawings showing proposed traffic control devices including temporary signage and temporary pavement markings and striping;
   ii. Different traffic diversion patterns and methods of control. Include for each phase detailed schedules for performance of work and include proposed traffic control devices;
   iii. Requirements for flagger training and qualifications, assignment, and supervision;
   iv. Notification plans for vehicular, bicycle, and pedestrian traffic detours including notifications of business owners, residents, and property owners in the vicinity of traffic and parking disruptions;
   v. Any other requirement of the authority having jurisdiction; and

l. Other safety and security elements as identified in the Contractor's corporate safety and security program.

1.2.4 Construction Site-Specific Health and Safety Plan Elements

The safety processes, equipment utilized, and personnel assignments to be provided by the Contractor at each individual work site may differ based upon a site-specific JHA performed by the Contractor. A SSHASP shall be developed for each distinct and unique work site. The SSHASP will be appropriate to the Project development, phasing, and tasks at hand. It may be submitted incrementally as work is designed and plans are approved for construction and will be revised as the Project evolves. A SONO of new or revised SSHASPs is required prior to the commencement of new work activities. Each SSHASP shall:

a. Be specific to the relevant work site conditions and Project phases for the Work;

b. Be kept on site and made available to all employees, authorized visitors, and the Authority upon request;

c. Include the Contractor's safety and security policy statement;

d. Conform to applicable workplace safety regulations including California Code of Regulations Title 8 Construction Safety Orders, FRA regulations as found at 49 C.F.R. Parts 214, 219, 225, 228, and 236; California Public Utilities Commission General Orders; Federal and State OSHA regulations;

e. Identify roles and responsibilities of all employees for the Contractor and Subcontractors with respect to safety;

f. Identify the reporting and inter-action processes of the Contractor's Safety team with the rest of the Project work force (including Subcontractors and the Authority), and with third parties such as emergency responders, utilities, and adjacent railroad operators;

g. Include a detailed description of site-specific hazards and mitigations. A daily JHA shall be conducted and a plan developed to alter mitigations as daily conditions change;

h. Include a detailed description of site-specific workplace health and safety rules and procedures that conform to all regulatory requirements described in the SSMP;

i. Include a detailed HAZWOPER Plan to be kept on site, available to all employees, authorized visitors, and the Authority upon request;

j. Roadway worker protection for adjacent railroad ROWs – Employees of any CRE working in these locations shall be trained by the Contractor to ensure they become fully familiar with railway operations, procedures, rules, and safety requirements;

k. Include a detailed plan for work site first-aid resources and a training program for employees;

l. Include a detailed Emergency Response Plan. The Emergency Response Plan shall be updated when conditions or procedures change. The Emergency Response Plan will be kept on site;

m. Include a detailed program for ensuring public safety at work sites and avoiding damage to public property, specific to each phase of the work;

n. Include a detailed Temporary Traffic Control Plan for each phase of the work; and

o. Include other elements that conform to the Contractor's corporate health and safety plan.

1.2.5 Site-Specific Security Plan Elements

Security at construction sites is to ensure all personnel working at the site, the Authority's assets and property, and the surrounding communities, are protected from trespassers, vandalism, theft, encroachment and other intentional criminal activity. In compliance with these provisions, the Contractor shall develop a SSSP which shall address crime and security- related conditions specific to the conditions and configuration of the individual work sites. This includes protection of property, materials, tools, equipment, and personal property of workers at specific sites. The SSSP will be appropriate to the Project development, phasing, and tasks at hand. The SSSP may be submitted incrementally as work is designed and plans are approved for construction, and will be revised as the Project evolves. A SONO of new or revised SSSPs is required prior to commencement of new work activities. The types of security to be provided by the Contractor at each site may differ based upon a site-specific security assessment performed by the Contractor.

The SSSP shall include:

a. Safety and security policy statement;

b. Threat and vulnerability assessment process, including how the process will be informed of threat conditions and how specific mitigations or controls will be applied to those potential threats of the construction areas;

c. Identification of the makeup, reporting structure, and inter-action processes of the Contractor's Project Management Team, including the Contractor's Security Management Team, with the rest of the Project work force (including Subcontractors and the Authority) and with third parties such as local law enforcement agencies;

d. Identification of security roles and responsibilities of all employees for the Contractor and Subcontractors;

e. Protection plan of public and property, materials, equipment, and tools based on the outcome of the security assessment through appropriate security applications such as fencing, access control, locks, alarms, intrusion detection, lighting, security guards, and any other security requirements that may be applicable;

f. A description of how access to individual worksites will control who and how employees access the specific sites, how other authorized persons are identified for each work site, and procedures for monitoring site specific access control performance;

g. Coordination program with local law enforcement for incident reporting, and other security-related conditions or events;

h. Procedures for providing site specific security information for inclusion into the Contractor's required project reporting requirements; and

i. Other elements that conform to the Contractor's corporate security plan or the SSMP.

1.2.6 Non-Compliance

The Contractor shall take all necessary corrective actions to avoid the issuance of a stop work order on identification of a safety or security noncompliance. If the Contractor fails or refuses to take corrective action promptly, the Authority may issue an order stopping all or part of the Work until satisfactory corrective action has been taken. The Contractor shall not base any claim or request for equitable adjustment for additional time or money on any stop order issued under these circumstances. The Contractor shall be responsible for its Subcontractors' compliance with this clause.

Appendix C

Safety & Security Policy Statement

TM 500.01

California High-Speed Train System

TECHNICAL MEMORANDUM

Safety and Security Policy Statement
TM 500.01

Prepared by:	John Cockle, System Safety	26 October 12 Date
Checked by:	Jack Sheehan, Safety & Security Manager	01 November 12 Date
Approved by:	Joseph Metzler, Operations Manager	07 November 12 Date
Released by:	Brent Felker, PE, Program Director	11-28-12 Date
Reviewed by:	Michael D. Lewis, PE, Project Management Oversight	07 NOV 12 Date
Reviewed by:	Jon Tapping, Risk Manager. Authority	11-16-12 Date
Accepted by:	Jeffrey Morales, CEO, Authority	12-7-12 Date

Revision	Date	Description
0	26 Oct 12	Initial Release

Note: Signatures apply for the latest technical memorandum revision as noted above.

Prepared by PARSONS BRINCKERHOFF

for the California High-Speed Rail Authority

TABLE OF CONTENTS

ABSTRACT

This memorandum is intended to establish the Safety and Security Policy for the California High-Speed Train System (CHSTS) that will be used as a confirmation of the California High-Speed Rail Authority's (Authority) commitment to plan, design, construct, test and prepare for operating a high-speed train system that operates with a primary focus on safety and security.

1.0 INTRODUCTION

The California High-Speed Rail Authority (Authority) is responsible for certifying the planning, design, construction, testing, and placement into revenue service a safe and secure high-speed train system. The Safety and Security Policy Statement is a high-level confirmation of the Authority's commitment to safety and security.

1.1 PURPOSE OF TECHNICAL MEMORANDUM

The purpose of this technical memorandum is to provide a vehicle for the authorization of the Safety and Security Policy Statement by the Authority.

1.2 GENERAL INFORMATION

Absent federal regulations that govern the completion of major capital projects, the Federal Railroad Administration looks to the Federal Transit Administration (FTA) regulations for guidance. FTA regulations found at 49 CFR 633 requires the development of a *Project Management Plan* (PMP) for every major capital transit project. As described in FTA Circular 5800.1 *Safety and Security Management Guidance for Major Capital Projects*, (dated 8/1/07) a *Safety and Security Management Plan* (SSMP) is the element of the PMP that manages project safety and security activities, responsibilities, and verification processes throughout the project life cycle.

A critical (and required) element of the SSMP, as described in FTA Circular 5800.1, is the Safety and Security Policy Statement.

2.0 DEFINITION OF TECHNICAL TOPIC

2.1 SAFETY AND SECURITY POLICY STATEMENT

It is the policy of the Authority to perform work on the California High-Speed Train System (CHSTS) in a manner that ensures the safety and security of passengers, employees, contractors, emergency responders, and the public. The application of system safety and security comprises a fundamental hazard and vulnerability management process that incorporates the characteristics of planning, design, construction, testing, operational readiness, and subsequent operation of the high-speed rail system. Safety and security are priority considerations in the planning and execution of all work activities on the CHSTS.

All trains, facilities, systems and operational processes must be designed, constructed, and implemented in a manner that promotes the safety and security of persons and property. The design, construction, testing, and start-up of the CHSTS will comply with applicable safety and security laws, regulations, requirements and railroad industry practices. The Authority will maintain or improve upon the public transit and railroad industry standards for safety and security. Through the Reliability, Availability, Maintainability, and Safety (RAMS) Program a standard of safety will be established that is as safe as or safer than conventional U.S. railroad operations and in conformance with the best practices and standards for safety in the international high-speed rail industry. The design, construction, testing, and start-up of the CHSTS will be accomplished in compliance with this standard.

The Authority is committed to providing a safe and secure travel and work environment. Therefore, safety, accident prevention, and security breach prevention must be incorporated into the performance of every employee task. All Authority, Program Management Team, and contractor personnel, subcontractors and employees are charged with the responsibility for ensuring the safety and security of passengers, employees, contractors, emergency responders, and the public who come in contact with the CHSTS. Each individual and organization is responsible for hazard and vulnerability management, for applying the processes that are designed to ensure safety and security, and for maintaining established safety and security standards, consistent with their position and organizational function. Through a cooperative team

effort and the systemic application of safety and security principles, the CHSTS will be designed, constructed, tested, and placed into service in a safe and secure manner.

3.0 SUMMARY AND RECOMMENDATIONS

3.1 RECOMMENDATIONS

It is recommended that the Authority approve and authorize this Safety and Security Policy Statement.

It is recommended that the Program Management Team implements this Safety and Security Policy Statement across all facets of the CHSTS, initially including it in the *Safety and Security Management Plan*, and subsequently in the *System Safety Program Plan* and the *Security and Emergency Preparedness Plan*.

It is recommended that the Safety and Security Policy Statement be included in all construction safety and security contract requirements.

It is recommended that the Authority's CEO signature be affixed to all versions of the Safety and Security Policy statement when published in other documents. See Appendix A.

APPENDIX A

Safety and Security Policy Statement

It is the policy of the California High-Speed Rail Authority (Authority) to perform work on the California High-Speed Train System (CHSTS) in a manner that ensures the safety and security of passengers, employees, contractors, emergency responders, and the public. The application of system safety and security comprises a fundamental hazard and vulnerability management process that incorporates the characteristics of planning, design, construction, testing, operational readiness, and subsequent operation of the high-speed rail system. Safety and security are priority considerations in the planning and execution of all work activities on the CHSTS.

All trains, facilities, systems and operational processes must be designed, constructed, and implemented in a manner that promotes the safety and security of persons and property. The design, construction, testing, and start-up of the CHSTS will comply with applicable safety and security laws, regulations, requirements and railroad industry practices. The Authority will maintain or improve upon the public transit and railroad industry standards for safety and security. Through the Reliability, Availability, Maintainability, and Safety (RAMS) Program a standard of safety will be established that is as safe as or safer than conventional U.S. railroad operations and in conformance with the best practices and standards for safety in the international high-speed rail industry. The design, construction, testing, and start-up of the CHSTS will be accomplished in compliance with this standard.

The Authority is committed to providing a safe and secure travel and work environment. Therefore, safety, accident prevention, and security breach prevention must be incorporated into the performance of every employee task. All Authority, Program Management Team, and contractor personnel, subcontractors and employees are charged with the responsibility for ensuring the safety and security of passengers, employees, contractors, emergency responders, and the public who come in contact with the CHSTS. Each individual and organization is responsible for hazard and vulnerability management, for applying the processes that are designed to ensure safety and security, and for maintaining established safety and security standards, consistent with their position and organizational function. Through a cooperative team effort and the systemic application of safety and security principles, the CHSTS will be designed, constructed, tested, and placed into service in a safe and secure manner.

Jeff Morales 12-5-12

Jeffrey Morales, CEO
California High-Speed Rail Authority

Date

Appendix D

Safety & Security Executive Committee Charter

TM 500.02

California High-Speed Train System

TECHNICAL MEMORANDUM

Safety and Security Executive Committee Charter
TM 500.02

Prepared by:	John Cockle, System Safety	26 October 12 Date
Checked by:	Jack Sheehan, Safety & Security Manager	01 November 12 Date
Approved by:	Joseph Metzler, Operations Manager	07 November 12 Date
Released by:	Brent Felker, Program Director	11-28-12 Date
Reviewed by:	Michael D. Lewis, PE, Project Management Oversight	07 NOV 12 Date
Recommended by:	Jon Tapping, Risk Manager	11-16-12 Date
Accepted by:	Jeffrey Morales, CEO	12.5.12 Date

Revision	Date	Description
0	26 Oct 12	Initial Release

Note: Signatures apply for the latest technical memorandum revision as noted above.

Prepared by PARSONS BRINCKERHOFF

for the California High-Speed Rail Authority

TABLE OF CONTENTS

ABSTRACT

The California High-Speed Rail Authority is responsible for planning, designing, constructing, testing and preparing for revenue operations a high-speed train system that is safe and secure. This responsibility is confirmed in the *Safety and Security Policy Statement*.

The Safety and Security Executive Committee allows the Authority to participate in the application of safety and security principles and processes to the California High-Speed Train System.

This memo is intended to establish the Safety and Security Executive Committee for the California High-Speed Train System in support of the *Safety and Security Management Plan*.

1.0 INTRODUCTION

The California High-Speed Rail Authority (Authority) is responsible for planning, designing, constructing, testing and preparing for revenue operations a high-speed train system that is safe and secure. The Safety and Security Executive Committee (SSEC) allows the Authority to participate in the application of safety and security principles and processes to the California High-Speed Train System (CHSTS).

1.1 PURPOSE OF TECHNICAL MEMORANDUM

The purpose of this technical memorandum is to define the scope, duties and responsibilities of the Safety and Security Executive Committee, identify committee membership and the members' respective responsibilities, and the process by which safety and security-related issues are addressed through the SSEC.

1.2 GENERAL INFORMATION

Absent federal regulations of its own that govern the completion of major capital projects, the Federal Railroad Administration (FRA) looks to the Federal Transit Administration (FTA) regulations for guidance. FTA regulations as stipulated at 49 CFR 633 require the development of a *Project Management Plan* (PMP) for every major capital transit project. As described in *FTA Circular 5800.1 Safety and Security Management Guidance for Major Capital Projects*, a *Safety and Security Management Plan* (SSMP) is the element of the PMP that details the processes for managing project safety and security activities, responsibilities, and verification processes throughout the project life-cycle.

A required element of the SSMP, as also described in FTA Circular 5800.1, is a description of committees identified to support the SSMP. The Committees may carry over to revenue operations through inclusion in the *System Safety Program Plan* and *Security and Emergency Preparedness Plan*. This SSEC Charter is designed to satisfy the requirement with respect to the Safety and Security Executive Committee.

2.0 DEFINITION OF TECHNICAL TOPIC

2.1 SSEC GOAL AND PURPOSE

The Safety and Security Executive Committee and its members will ensure that the CHSTS is designed, built, and implemented in a safe and secure manner. The SSEC will achieve this goal by providing oversight of the application of the SSMP through all phases of the CHSTS development and to act as a conduit to informing and assuring Authority executive management of safety and security issues affecting the CHSTS.

2.2 AUTHORITY

The authority for the Safety and Security Executive Committee is established in the *Safety and Security Management Plan* (SSMP). The SSEC Charter will be modified as necessary as the development of the CHSTS progresses.

2.3 SCOPE

The Safety and Security Executive Committee will address safety and security issues which:

- Are Authority policy considerations;
- Require Authority approval;
- Require Authority direction for resolution of a dispute; or,
- Constitute final acceptance of Safety and Security Certification.

2.4 DUTIES AND RESPONSIBILITIES

The duties and responsibilities of the Safety and Security Executive Committee are as follows:

- Approve the initial version of the SSMP and subsequent updates
- Oversee the application of the SSMP through all CHSTS development phases
- Authorize the establishment of the Safety and Security Project Committee (SSPC), comprised of members of the Program Management Team (PMT)
- Review and approve regular reports of safety and security activities from the SSPC
- Resolve safety and security issues that cannot be resolved at the SSPC level
- Review and approve Safety and Security Certification (SSC) Certificates of Conformance and a final Certification Verification Report prior to the start of applicable testing phases or startup of revenue service
- Provide a forum for safety and security discussions among Authority and PMT Executive Management

2.5 MEMBERSHIP

The Safety and Security Executive Committee comprises the following persons:

- Authority Executive Director (Chairperson)
- Authority Safety and Security Representative
- Authority Regional Directors
- Authority Chief Program Manager
- Authority Chief Counsel
- PMT Program Director
- PMT System Safety Manager (Committee Secretary)
- PMT System Security Manager

The Chairperson of the SSEC is the Authority Executive Director or a designated Authority executive management representative. If a designated member of the SSEC is unable to attend a SSEC meeting, they must assign an appropriate representative.

2.6 MEETINGS

The Safety and Security Executive Committee will meet at least quarterly at a regular time and location determined at the previous meeting. The Chairperson (or designee) will conduct the meeting according to the published agenda. The meeting may be postponed or rescheduled by the Chairperson due to the availability of the membership.

The PMT System Safety Manager will act as Secretary and will be responsible to notify all SSEC members of the time, date, location, and agenda in advance of the meeting. The Secretary will also distribute any support material pertinent to the meeting.

To validate meetings and the business conducted therein, a quorum of members must be present at the meeting. A quorum is a simple majority of the membership.

Special meetings may be called on an exceptional basis at the direction of the Chair or designee to discuss matters of urgency. In these cases, the Secretary will notify all members in writing of the date, time, place and purpose of the meeting at least 48 hours in advance if possible.

The Secretary will record all proceedings of the Committee and maintain an action items matrix showing resolutions and pending items. The Chairperson will designate a person responsible for follow up of the action items as required.

The Secretary will distribute meeting minutes, an action items matrix, and supporting forms to all SSEC members via e-mail within one week following each meeting. Members have one week to

advise the Secretary of any inaccuracies. A copy of meeting minutes, an action items matrix, and supporting forms shall be retained by the SSEC Secretary in accordance with the Authority's Record Retention Policy.

3.0 SUMMARY AND RECOMMENDATIONS

3.1 RECOMMENDATIONS

It is recommended that the California High-Speed Rail Authority approve and authorize this Safety and Security Executive Committee Charter.

It is recommended that the PMT implement this SSEC Charter by appending it to the *Safety and Security Management Plan.*

It is recommended that this SSEC Charter be appended to both the *System Safety Program Plan* and the *Security and Emergency Preparedness Plan* (when they are developed) prior to the initiation of revenue service.

Appendix E

Safety & Security Program Committee Charter

TM 500.03

California High-Speed Train System

TECHNICAL MEMORANDUM

Safety and Security Program Committee Charter
TM 500.03

Prepared by:	John Cockle, System Safety	July 26, 2013
Checked by:	Lurae Stuart, Security Manager	July 29, 2013
Approved by:	Joseph Metzler, Operations Manager	July 29, 2013
Released by:	Teri Zink, Interim Program Director	July 30, 2013

Revision	Date	Description
0	26 OCT 2012	Initial Release
1	26 JUL 2013	Update for SSPC Membership

Note: Signatures apply for the latest technical memorandum revision as noted above.

Prepared by PARSONS BRINCKERHOFF

for the California High-Speed Rail Authority

TABLE OF CONTENTS

ABSTRACT

The California High-Speed Rail Authority is responsible for planning, designing, constructing, testing and preparing for operating a high-speed train system that is safe and secure. This responsibility is confirmed in the *Safety and Security Policy Statement*.

The Safety and Security Executive Committee allows the Authority to participate in the application of safety and security principles and processes to the development of the California High-Speed Train System through the Safety and Security Program Committee, which operates at the project level.

This memo is intended to establish the Safety and Security Program Committee for the CHSTS in support of the *Safety and Security Management Plan*.

1.0 INTRODUCTION

The California High-Speed Rail Authority (Authority) is responsible for planning, designing, constructing, testing and preparing for revenue operations of a high-speed train system that is safe and secure. Under the direction of the Authority, the Program Management Team (PMT) is responsible for carrying out the safety and security initiatives that are described in the *Safety and Security Management Plan* (SSMP).

The Safety and Security Project Committee (SSPC) allows the PMT to implement the SSMP throughout the California High-Speed Train System (CHSTS).

1.1 PURPOSE OF TECHNICAL MEMORANDUM

The purpose of this technical memorandum is to define the scope, duties and responsibilities of the Safety and Security Program Committee, identify committee membership and the members' respective responsibilities, and the process by which safety and security-related issues are addressed through the SSPC.

1.2 GENERAL INFORMATION

Absent federal regulations that govern the completion of major capital projects, the Federal Railroad Administration looks to the Federal Transit Administration (FTA) regulations for guidance. FTA regulations as stipulated at 49 CFR 633 require the development of a *Project Management Plan* (PMP) for every major capital transit project. As described in *FTA Circular 5800.1 Safety and Security Management Guidance for Major Capital Projects*, a *Safety and Security Management Plan* (SSMP) is the element of the PMP that details the processes for managing project safety and security activities, responsibilities, and verification processes throughout the project life-cycle.

A required element of the SSMP, as also described in FTA Circular 5800.1, is a description of committees identified to support the SSMP. The Committees may carry over to revenue operations through inclusion in the *System Safety Program Plan* and *Security and Emergency Preparedness Plan*. This SSPC Charter is designed to satisfy the requirement with respect to the Safety and Security Program Committee.

2.0 DEFINITION OF TECHNICAL TOPIC

2.1 SSPC GOAL AND PURPOSE

The Safety and Security Program Committee and its members will ensure that the CHSTS is designed, built, and implemented in a safe and secure manner at the project level. The SSPC will achieve this goal by providing oversight of the application of the SSMP through all phases of CHSTS development and to act as a conduit to informing and assuring Authority executive management (through the Safety and Security Executive Committee) of safety and security issues affecting the CHSTS.

2.2 AUTHORITY

The authority for the Safety and Security Program Committee is established in the *Safety and Security Management Plan* (SSMP). The SSPC Charter will be modified as necessary as CHSTS development progresses.

2.3 SCOPE

The Safety and Security Program Committee will address safety and security issues which:

- Are directed it by the SSEC;
- Are appropriate for or require resolution at the Program level;
- Require elevation to the SSEC for Authority direction for resolution; or,
- Constitute preliminary review and approval of Safety and Security Certification.

2.4 DUTIES AND RESPONSIBILITIES

The duties and responsibilities of the Safety and Security Program Committee are as follows:

- Recommend to the Safety and Security Executive Committee (SSEC) the initial version of the SSMP and subsequent updates
- Oversee the application of the SSMP through all CHSTS development phases
- Review and forwarding to the SSEC with recommendation for approval of Preliminary Hazard Analyses and Threat/Vulnerability Assessments as they are developed or updated
- Tracking of identified hazards or vulnerabilities through the hazard/vulnerability tracking database
- Provide regular reports of safety and security activities to the SSEC
- Forward to the SSEC for resolution any safety and security issues that cannot be resolved at the SSPC level
- Review of Safety and Security Certification (SSC) Certificates of Conformance and a Final Certification Verification Report
- Forward SSC Certificates of Conformance and a final Certification Verification Report with recommendation to the SSEC for Authority acceptance prior to the start of applicable testing phases or startup of revenue service
- Provide a forum for safety and security discussions among PMT staff members and a conduit for safety and security issues to the Authority through the SSEC

2.5 MEMBERSHIP

The Safety and Security Project Committee comprises the following persons:

- Authority Safety and Security Manager (Committee Chairperson)
- Authority Deputy Chief Program Manager
- PMT System Safety Manager (Committee Secretary)
- PMT System Security Manager
- PMT Program Director
- PMT O&M Manager
- PMT Engineering Manager
- PMT Systems Engineering Manager
- PMT Construction Manager
- PMT Project Risk Manager
- PMT RAMS Manager

Designated members of the SSPC are responsible for assigning an appropriate representative if they are unable to attend a SSPC meeting.

2.6 MEETINGS

The Safety and Security Program Committee will meet at least monthly at a regular time and location. The Chairperson (or designee) will conduct the meeting according to the published agenda. The meeting may be postponed or rescheduled by the Chairperson due to the availability of the membership.

The Secretary will be responsible for notifying all SSPC members of the time, date, location, and agenda in advance of the meeting. The Secretary will also distribute any support material pertinent to the meeting.

To validate meetings and the business conducted therein, a quorum of members must be present at the meeting. A quorum is a simple majority of the membership.

Special meetings may be called on an exceptional basis at the direction of the Chairperson or his/her designated representative to discuss matters of urgency. In these cases, the Secretary will notify all members in writing of the date, time, place and purpose of the meeting at least 48 hours in advance if possible.

The Secretary will record all proceedings of the Committee and maintain an action items matrix showing resolutions and pending items. The Chairperson will designate a person responsible for follow up of the action items as required.

The Secretary will distribute meeting minutes, an action items matrix, and supporting forms to all SSPC members via e-mail within one week following each meeting. Members have one week to advise the Secretary of any inaccuracies. A copy of meeting minutes, an action items matrix, and supporting forms shall be retained by the Secretary in accordance with the Authority's Record Retention Policy.

3.0 SUMMARY AND RECOMMENDATIONS

3.1 RECOMMENDATIONS

It is recommended that the California High-Speed Rail Authority approve and authorize this Safety and Security Program Committee Charter.

It is recommended that the PMT implement this SSPC Charter by appending it to the *Safety and Security Management Plan*.

It is recommended that this SSPC Charter be appended to both the *System Safety Program Plan* and the *Security and Emergency Preparedness Plan* (when they are developed) prior to the initiation of revenue service.

Appendix F

Fire & Life Safety and Security Program

TM 500.04

California High-Speed Train System

TECHNICAL MEMORANDUM

Fire and Life Safety and Security Program
TM 500.04

Prepared by:	John Cockle, System Safety	26 October 12 Date
Checked by:	Jack Sheehan, Safety & Security Manager	01 November 12 Date
Approved by:	Joseph Metzler, Operations Manager	07 November 12 Date
Released by:	Brent Felker, PE, Program Director	11-28-12 Date
Reviewed by:	Michael D. Lewis, PE, Project Management Oversight	07 Nov 12 Date
Reviewed by:	Jon Tapping, Risk Manager , Authority	11-16-12 Date
Accepted by:	Jeffrey Morales, CEO, Authority	12.5.12 Date

Revision	Date	Description
0	26 Oct 2012	Initial Release, R0

Note: Signatures apply for the latest technical memorandum revision as noted above.

Prepared by PARSONS BRINCKERHOFF

for the California High-Speed Rail Authority

RFP No.: HSR 13-57 – Addendum No. 2 - 06/30/2014

TABLE OF CONTENTS

ABSTRACT

This Technical Memorandum (TM) establishes the Fire and Life Safety and Security Program, including the establishment of Regional and System Fire and Life Safety and Security Committees.

1.0 PURPOSE

The purpose of this Technical Memorandum (TM) is to establish the approach the California High-Speed Rail Authority (Authority) will take with respect to fire and life safety and security issues in the development and implementation of the California High-Speed Train System (CHSTS), and to provide a medium for the authorization of the Fire and Life Safety and Security Committees.

2.0 BACKGROUND

The identification of design criteria that specifically addresses fire and life safety issues is a critical component of the development and operation of passenger rail transit systems. Involving emergency response agencies (both systemically and locally) in the development of fire and life safety design criteria and operating practices assures the Authority and the passenger railroad operator that emergency response infrastructure, equipment and procedures are designed, constructed/installed, and implemented to an acceptable level of safety.

Security has been added to the traditional fire and life safety scope in order to bring together all local emergency response agencies into one forum. This strategy allows the Authority to capitalize on commonalities among emergency response agencies as a force multiplier, increasing lines of communication while maximizing CHSTS resources.

Absent federal regulations that govern the completion of major capital projects for railroad systems, the Federal Railroad Administration looks to the Federal Transit Administration (FTA) regulations for guidance. FTA regulations as stipulated at 49 CFR 633 require the development of a *Project Management Plan* (PMP) for every major capital transit project. As described in *FTA Circular 5800.1 Safety and Security Management Guidance for Major Capital Projects*, a *Safety and Security Management Plan* (SSMP) is the element of the PMP that details the processes for managing project safety and security activities, responsibilities, and verification processes throughout the project life-cycle.

A required element of the SSMP, as also described in FTA Circular 5800.1, is a description of committees identified to support the SSMP. The Committees may carry over to revenue operations through inclusion in the *System Safety Program Plan* and *Security and Emergency Preparedness Plan*. This Fire and Life Safety and Security Program is designed to satisfy the requirement with respect to the Fire and Life Safety and Security Committees.

3.0 FIRE AND LIFE SAFETY AND SECURITY PROGRAM

3.1 Purpose

The purpose of the Fire and Life Safety and Security (FLSS) Program is to assure that fire and life safety and security considerations are integrated into the CHSTS design criteria, programs, procedures, and communications to the maximum extent possible.

Fire and Life Safety and Security Committees (FLSSC) will be established for the purpose of engaging emergency response agencies, at both state and regional levels, to acquire their input with regard to CHSTS designs that mitigate identified hazards. The FLSSC are essential to fostering a professional, friendly, collaborative relationship with the local emergency response agencies, helping to facilitate final permit approval and issuance of Certificates of Occupancy for successful implementation of revenue service. The goal of these committees is to provide a forum for emergency response agencies to provide input and feedback to the Authority concerning fire and life safety and security issues in a formal and consistent manner.

3.2 Scope

The scope of the FLSSC during the Planning, Preliminary Engineering and Final Design project phases will focus on infrastructure and systems design requirements. For the CHSTS, security is added to the traditional fire and life safety scope in order to bring together all local emergency response agencies to one forum. Operational procedures, emergency response procedures, and training requirements and exercises will be considered by the FLSSC during the Construction and Testing/Startup project phases.

Security will remain an integral part of the FLSS Program during the Planning, Preliminary Engineering and Final Design project phases. Separate Security Committees may be established when considered appropriate by the Authority.

Two approaches are executed for the Fire and Life Safety and Security Committees: Regional Committees and a Statewide Committee to address state-level issues.

The Authority's safety and security managers will have primary responsibility for administering the FLSS Program including interactions with local, regional, and statewide emergency response agencies, and holding chairperson positions within the various FLSS committees.

3.2.1 Statewide FLSSC

The one Statewide FLSSC will focus on systemic, high-level, fire and life safety and security issues including Federal and State codes or requirements impacting the regional efforts. A goal of the Statewide FLSSC is to obtain concurrence from federal and state authorities with respect to fire and life safety and security concerns.

The Statewide FLSSC will include representatives from state and federal agencies such as the Office of the State Fire Marshal, California Highway Patrol, Office of Emergency Services, the California Emergency Management Agency, CPUC, FRA, and DHS as well as a representative from each Regional FLSSC. The Statewide FLSSC will be chaired by the Authority's Safety and Security Manager(s). Meetings will be held regularly in Sacramento with agendas, minutes, and other support materials supplied by the committee Chair. Minutes and action items from the meetings will be conveyed to the Regional FLSSC's and to the Safety and Security Program Committee for their consideration. It is anticipated that these Statewide FLSSC meetings will be held quarterly.

3.2.2 Regional FLSSC

Each Regional FLSSC will focus on the CHSTS characteristics specific to their corridor segments (type/length of underground and elevated structures, access methods, terminals, etc.) to provide input with respect to local building codes or requirements that are in line with the emergency response characteristics and capabilities of the local agencies. A goal of the Regional FLSSC is to obtain concurrence from local emergency response agencies with respect to the proposed designs and the code requirements of the state and federal authorities having jurisdiction.

The Regional FLSSC will be comprised of appropriate representatives (e.g., Fire Marshal) from local emergency response agencies (fire, police, emergency medical response) and will be chaired by the Authority's Safety and Security Manager(s), and include the Authority's Regional Director for the region. Meetings will be held regularly at a location local to the regional corridor, with agendas, minutes, and other support materials supplied by the committee Chair. Minutes and action items from the meetings will be conveyed to the Statewide FLSSC and to the Safety and Security Program Committee for their consideration. It is anticipated that these Regional FLSSC meetings will be held quarterly initially, alternating with the Statewide FLSSC. Frequency will be increased as the need dictates.

One representative from each Regional FLSSC will be asked to participate in the Statewide FLSSC. Consistent representation is critical to success. Each Regional representative must be the same representative attending to Statewide FLSSC matters and reporting results to their specific Regional Committee.

3.3 Fire and Life Safety and Security Report

The input gathered through the FLSSC will support the development of Preliminary Hazard Analysis, Threat and Vulnerabilities Assessments, and other analyses as required and in conformance with the CHSTS Safety and Security Management Plan. The results of these analyses will be used to develop safety and security design criteria and operational procedures, all of which will be assured through the Verification & Validation process. A Fire and Life Safety and Security Report will be developed to describe the system-level strategies, mitigations, and processes implemented to achieve an acceptable level of fire and life safety. The Fire and Life Safety and Security Report will be updated as conditions change or as new information is acquired through the FLSSC.

4.0 POLICY RECOMMENDATION

It is recommended that Authority implement a Fire and Life Safety and Security Program for the CHSTS by appending this Technical Memorandum to the CHSTS Safety and Security Management Plan (SSMP). It is also recommended that this Technical Memorandum is appended to both the System Safety Program Plan (SSPP) and Security and Emergency Preparedness Plan (SEPP) when they are developed prior to the initiation of revenue service.

It is recommended that Regional FLSSCs be established in the Initial Construction Segment between Fresno and Bakersfield. It is also recommended that the Statewide FLSSC be established in Sacramento, California. All committees should be established as soon as possible in order to integrate FLSS input to the development of design criteria.

This Policy will be modified as design and construction progresses to fit the specific needs of the immediate phase of the project segments.

Appendix G

Hazard Analysis Descriptions

Preliminary Hazard Analysis (PHA)

The primary output of the PHA is the early identification and evaluation of hazards and mitigations on a high-level systems requirement basis. The following instructions are used in the development of the Preliminary Hazard Analysis:

PURPOSE	The purpose of the PHA is to provide an early assessment of the hazards associated with a design or concept.
PROCEDURE	The PHA identifies critical areas, hazards and criteria being used and considers: hazardous events, components, interfaces, environmental constraints, and operating, maintenance and emergency procedures. When possible, the corrective action should identify the approach(s) to be taken: design change, procedures, and special training and personnel qualifications.
RESULTS	The PHA will provide for verification that corrective or preventive measures or procedures are taken in safety reviews, modification of specifications, and generation of methods and procedures to eliminate, minimize or control hazards and provide inputs to the interface hazard analysis, operating hazard analysis and failure mode and effects analysis.
DOCUMENTATION	Document the analysis to show compliance with the specified safety and operational requirements, and provide for the tracking of actions and verifying effectiveness. A PHA Report will be developed where appropriate to document the analysis process for specific subsystem hazards.

Sample PHA

System: Infrastructure				**California High-Speed Train Project**				**Prepared by:** John Cockle **Date** 5-Feb-14		
Subsystem: R-O-W, Generally				**Preliminary Hazard Analysis (PHA)**				**Reviewed by:** Gulzar Ahmed **Date** 5-Feb-14		
PHA No. 1.1.1 **Rev No.** 0								**Approved by:** **Date**		
General Description Derailment				**Hazard Cause / Effect**		**Hazard Risk Index**		**Corrective Action**		
No.	**Sys Mode**	**Site Specific**	**Hazard Description**	**Potential Cause**	**Effect on Subsystem / System**	**Initial**	**Residual (Projected)**	**Potential Controlling Measures**	**Resolution**	**Remarks**
4	Normal	Yes	Washout	Flooding, scouring	Derailment w/mass casualties, property damage, service interruption	I-B Unacceptable	I-E Acceptable w/Review	1) Perform hydraulics analysis and incorporate results into sub-grade design, slope protection and setting of profile. 2) Install scour protection (revetment or other structure) to protect sub-grade from water course. 3) Install culvert or bridge structure where crossing water course. 4) Identification and monitoring by O&M of potential hazardous locations.	1) Perform hydraulics analysis and incorporate results into sub-grade design, slope protection and setting of profile. 2) Install scour protection (revetment or other structure) to protect sub-grade from water course. 3) Install culvert or bridge structure where crossing water course. 4) Identification and monitoring by O&M of potential hazardous locations.	Identified 8/30/11. Improvement in frequency to *Highly Unlikely*, but not eliminated. No effect on severity of a derailment if it does occur. 12/2013: Mitigation and Resolution # 4 added during the Verification and Validation process

Note – This is a sample representation only. Refer to current PHA for identified hazards and controlling measures.

INSTRUCTIONS FOR COMPLETING THE PHA FORM:

- In System, enter the nomenclature of the applicable system element (e.g. Infrastructure, Train Control, Communications, Rolling Stock, etc).

- In Subsystem, enter the nomenclature of the subsystem as broken out from the system and which includes the item or hazard undergoing PHA.
- In PHA No., enter the PHA number for the subsystem element. This coding will be sequentially numbered by each Contractor for each subsystem and will be utilized for all related analysis.
- In Rev. No., enter the revision number of the PHA to indicate the latest status.
- In Prepared by _ Date _, the preparer will sign and enter the date of issue or revision of the analysis.
- In Reviewed by _ Date _, the reviewer will enter the date of review.
- In Approved by _ Date _, enter the date of approval by the SSPC or SSEC as appropriate.
- In No., enter the reference number which uniquely identifies the high-speed rail system element and any identifiable element subsystem and item being analyzed.
- In System Mode, enter state of the system when the failure mode or hazardous condition occurs.
- In HAZARD DESCRIPTION, describe an immediate condition which could lead to an accident involving potential injury, death or equipment damage.
- In POTENTIAL CAUSE, enter the most likely primary and secondary causes that can potentially contribute to the presence of the hazard.
- In EFFECT ON SUBSYSTEM / SYSTEM, describe the effect that the hazardous condition may have on the system element or its element subsystem in terms of safety (e.g. delay, inconvenience, injury, damage, fatality, etc.)
- In HAZARD RISK INDEX, enter a combination of the qualitative measure of the worst potential consequence resulting from the hazard, and its probability of occurrence (e.g., IA, IIB, etc.), under the following conditions:
    - In INITIAL, enter the designation for hazard risk index estimated prior to implementation of the controlling measures, considering the condition of the subsystem element if no measures of mitigation were applied.
    - In RESIDUAL (PROJECTED), enter the designation for hazard risk index estimated following the adoption/implementation of the proposed controlling measures. This may result in reduction of either the probability of occurrence or the severity of the hazard, or both.
- In POTENTIAL CONTROLLING MEASURES AND REMARKS, describe the proposed measures of mitigation that can be applied to prevent or reduce the severity and probability of the hazard under analysis.
- In RESOLUTION / RESOLUTION, describe changes made or steps taken relative to design and/or procedures, training, etc., to eliminate or control the hazard. The identified reference should be as specific as possible for verification purposes.
- In REMARKS, identify the date that the hazard was initially analyzed, any subsequent analysis, and other items that support or describe the analysis process.

Site-Specific Hazard Analysis (SiSHA)

The SiSHA is conducted as the general design criteria and system requirements are applied to specific system and subsystem elements within a defined geographic area. The standard SiSHA segment will be one mile in length, but can be shorter if specialized conditions require. SiSHA is systemic in that it includes ALL hazards and mitigations that are found within the segment under consideration, analyzing the relationship between the various hazards and mitigations. SiSHA is performed when the final alignment is identified during the Preliminary Engineering Phase and in advance of the Final Design, Construction, and Testing/Startup Phases. The primary output of the SiSHA is a validation of the PHA mitigations in relation to the segment under consideration, and the identification and evaluation of hazards and mitigations that are specific to the segment under consideration.

The instructions and format for completing the SiSHA form are the same as for the PHA form.

Failure Mode and Effects Analysis (FMEA)

PURPOSE

The purpose of the FMEA is to determine the results or effects of item failures on a system operation and to classify each potential failure according to its risk index (severity and frequency of occurrence). The goal is to provide an early identification of failures with unacceptable and undesirable risks so that they can be eliminated or minimized through appropriate actions at the earliest possible time.

PROCEDURE

Variations in design complexity and available data will generally dictate the analysis approach to be used. There are two primary approaches for accomplishing an FMEA, the hardware approach and the functional approach.

The hardware approach is normally used when hardware items can be uniquely identified from schematics, drawings, and other engineering and design data. The hardware approach is normally utilized in a parts-level up fashion (bottom-up approach); by listing individual hardware items and analyzing the effect of their possible failure modes on the entire system and its subsystems.

The functional approach is normally used when hardware items cannot be uniquely identified or when system complexity requires analysis from the initial indenture level downward through succeeding indenture levels (top-down approach). The functional approach recognizes that every item is designed to perform a number of functions that can be classified as outputs. The outputs are listed and their failure modes analyzed.

The FMEA may be performed as a hardware analysis, a functional analysis, or a combination analysis depending on the design detail available.

The FMEA will examine the system element by element, to evaluate the system for safety hazards and ultimately to assess risk. Each identified failure mode will be assigned a severity classification. A probability of occurrence will also be assigned in accordance with MIL-STD-882E The resulting risk index will be utilized during design to establish priorities for corrective actions. The FMEA will be reviewed on a continuous basis to verify that design modifications do not add hazards to the system.

To perform a FMEA, the following process should be implemented:

- Identify all major system components, functions, and processes
- Determine consequences of interest
- Determine the potential failure modes of interest
- Specify effects of failures of system
- Identify safety provisions to control hazards and failures
- Identify detection methods for failures
- Establish overall significance of each failure

RESULTS	The FMEA will provide information to evaluate identified hazards, identify safety critical areas and provide inputs to safety design criteria and procedures with provisions and alternatives to eliminate or control all unacceptable and undesirable hazards based on their combination of severity and probability of occurrence, and to identify critical items.
DOCUMENTATION	Document the analysis to show compliance with specified system safety requirements and to track the corrective action.

Fault Tree Analysis (FTAn)

PURPOSE

The Fault Tree Analysis (FTAn) is a deductive procedure used to determine the various combinations of hardware and software failures and human errors that could cause undesired events (referred to as top events) at the system level. The FTAn has much use because of its ability to distinguish between those events that must occur (represented by an AND gate) and those that simply can occur (represented by an OR gate) in order for the top event to occur. The analysis thus helps to identify potential causes of system failures before the failures actually occur. The deductive analysis begins with a general conclusion, then attempts to determine the specific causes of the conclusion by constructing a logic diagram called a fault tree. After completing an FTAn, efforts can be directed to improve system safety.

PROCEDURE

The FTAn will be conducted on unresolved, undesirable, or unacceptable hazards identified in other safety analyses. Following procedure will be used to do a comprehensive FTAn:

1. Define the undesirable/unacceptable hazard, and write down the top level event.
2. Using technical information and professional judgments, determine the possible reasons for the top level event to occur. These are level two elements because they fall just below the top level event in the tree.
3. Continue to break down each element with additional gates to lower levels. Consider the relationships between elements to help decide proper selection of the logic gate.
4. .Finalize and review the complete diagram. The chain can only be terminated in a basic fault: human, hardware software.
5. If possible, evaluate the probability of occurrence for each of the lowest level elements and calculate the statistical probabilities from the bottom up.

RESULTS

The information charted on a fault tree provides a qualitative analysis by demonstrating how specific events will affect an outcome. If probability data is known for these events, then the FTAn can also provide quantitative information to further evaluate the likelihood of achieving the top event. Once developed, the fault areas that are responsible for yielding an undesired event can be further evaluated.

DOCUMENTATION

Document the analysis to show compliance with specified system safety requirements and to track the corrective action.

Interface Hazard Analysis (IHA)

PURPOSE	The IHA identifies and assesses existing or potential hazards between subsystems and systems and their effect on overall System safety and operations. The emphasis is on interfaces. Through the early identification of existing or potential hazards, corrective action(s) can be taken to eliminate or control unacceptable and undesirable hazards, based on the combination of their hazard severity and probability of occurrence.
PROCEDURE	The IHA is conducted on the critical interrelationships of each subsystem and system to determine the cause and effect of possible independent, dependent and simultaneous failures that could present a hazardous condition, including failures of safety devices. When the IHA indicates a potential problem, it is made known to the responsible engineer in order to initiate a design review. The IHA will be reviewed on a continuous basis to verify that design modifications do not add hazards to the system.
RESULTS	The IHA provides for the identification and correction of possible hazards associated with subsystem and system failures. The IHA provides inputs to design reviews, maintainability, reliability and system safety and system operations.
DOCUMENTATION	Document the analysis to show compliance with specified system safety requirements and to track the corrective action.

Operating Hazard Analysis (OHA)

PURPOSE	The purpose of the OHA is to identify and analyze hazards associated with personnel and procedures during production, installation, testing, training, operations, maintenance and emergencies.
PROCEDURE	The OHA will be conducted on all tasks and human actions, including acts of omission and commission, by persons interacting with the system, subsystems and assemblies at any level. When the OHA indicates a potential safety hazard, it will be made known to the responsible engineer, in order to initiate a design review or a system safety working group action item. The OHA will be reviewed on a continuous basis to provide for design modifications, procedures, testing, etc., that do not create hazardous conditions.
RESULTS	The OHA will provide for corrective or preventive measures to be taken to minimize the possibility that any human error or procedure will result in injury or system damage. The OHA will provide inputs for recommendations for changes or improvements in design or procedures to improve efficiency and safety, development of warning and caution notes to be included in manuals and procedures, and the requirement of special training of personnel who will carry out the operation and maintenance of the system.
DOCUMENTATION	Document the analysis to show compliance with specified system safety and operational requirements.

Software Hazard Effects Analysis (SHEA)

PURPOSE

The Software Hazard Effects Analysis (SHEA) is a software design evaluation and validation tool used to identify errors generated from incorrect or inadequate specifications of software functions. A software fault causing a resultant harmful system function is a software hazard.

Software faults can be described in three forms:

- Error generated through coding the software
- Faults due to incorrect software specifications implemented by the function developer
- Faults due to hardware failures that affect changes in coding software

A software hazard can be any of four types:

- An undesired signal causing an unwanted event
- An undesired signal causing an out-of-sequence event in the response
- An undesired signal preventing the occurrence of a necessary action or response
- An undesired signal causing an event to be out of tolerance

The SHEA concentrates on potential safety problem areas in the software. The purpose of the SHEA is to provide an early study of the software design for possible hazards and to initiate appropriate actions to eliminate/ control hazards.

PROCEDURE

The initial step in the analysis is to identify the safety critical areas of the system and their functional paths. These paths may contain hardware as well as software elements. Focus the analysis on the software functions within each system functional flow path. Whether the coded instructions are stored in software or firmware, analysis of the system in question for hazardous occurrences should include an analysis of the stored coded instructions.

The SHEA will be conducted on identified software fault conditions, and will proceed from a qualitative to a quantitative analysis as the design develops. When the SHEA indicates a potential problem, it will be made known to the responsible engineer in order to initiate proper action. The SHEA will be reviewed on a continuous basis to verify that software design modifications do not add hazards to the system.

The SHEA should be developed in conjunction with FMEA.

RESULTS

The SHEA will provide information to evaluate identified software related hazards, identify safety critical areas in software design and provide inputs to safety design criteria and procedures. The latter will include provisions and alternatives to eliminate or control all unacceptable and undesirable software related hazards based on their combination of severity and probability of occurrence, and to identify critical items.

DOCUMENTATION

Document the analysis to show compliance with the specified system safety requirements and to track the corrective action.